Red Hat Enterprise Linux 3

Referenzhandbuch

Red Hat Enterprise Linux 3: Referenzhandbuch
Copyright © 2003 von Red Hat, Inc.

Red Hat, Inc.

1801 Varsity Drive Raleigh NC 27606-2072 USA Phone: +1 919 754 3700 Phone: 888 733 4281 Fax: +1 919 754 3701 PO Box 13588 Research Triangle Park NC 27709 USA

rhel-rg(DE)-3-Print-RHI (2003-07-25T17:13)
Copyright © 2003 by Red Hat, Inc. Das vorliegende Material darf nur unter Einhaltung der in Open Publication License, V1.0 oder neuer dargelegten Geschäftsbedingungen vertrieben werde (die neueste Version ist gegenwärtig unter http://www.opencontent.org/openpub/ verfügbar).
Beträchtlich modifizierte Versionen dieses Dokumentes dürfen nur mit ausdrücklicher Genehmigung des Copyright-Inhabers vertrieben werden.
Der Vertrieb des Werks oder einer Ableitung des Werks in Standardbuchform (Papier) zu kommerziellen Zwecken ist nicht zulässig, sofern dies nicht zuvor durch den Copyright-Inhaber genehmigt wurde.
Red Hat, Red Hat Network, das Red Hat "Shadow Man" Logo, RPM, Maximum RPM, das RPM Logo, Linux Library, PowerTools, Linux Undercover, RHmember, RHmember More, Rough Cuts, Rawhide und alle Red Hat-basierten Warenzeichen und Logos sind Warenzeichen oder eingetragene Warenzeichen von Red Hat, Inc. in den USA und anderen Ländern.
Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.
Motif und UNIX sind eingetragene Warenzeichen von The Open Group.
Intel und Pentium sind eingetragene Warenzeichen der Intel Corporation. Itanium und Celeron sind Warenzeichen der Intel Corporation.
AMD, Opteron, Athlon, Duron und K6 sind eingetragene Warenzeichen von Advanced Micro Devices, Inc.
Netscape ist ein eingetragenes Warenzeichen der Netscape Communications Corporation in den USA und anderen Ländern.
Windows ist ein eingetragenes Warenzeichen der Microsoft Corporation.
SSH und Secure Shell sind Warenzeichen der SSH Communications Security, Inc.
FireWire ist ein Warenzeichen der Apple Computer Corporation.
IBM, AS/400, OS/400, RS/6000, S/390 und zSeries sind eingetragene Warenzeichen der International Business Machines Corporation. eServer, iSeries und pSeries sind Warenzeichen der International Business Machines Corporation.
Alle weiteren hier genannten Rechte an Warenzeichen sowie Copyrights liegen bei den jeweiligen Eigentümern.
Der GPG-Code des security@redhat.com Schlüssels lautet:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Inhaltsverzeichnis

Einführung ..... **i**
1. Änderungen an diesem Handbuch i
2. So finden Sie die geeignete Dokumentation ii
2.1. Dokumentation für Linux-Einsteiger ii
2.2. Für erfahrene Linux-Benutzer. iv
2.3. Dokumentation für Linux-Gurus v
3. Dokumentkonventionen v
4. Verwenden der Maus viii
5. Kopieren und Einfügen von Text mit X viii
6. Fortsetzung folgt! viii
6.1. Wir brauchen Ihre Rückmeldung! ix
7. Melden Sie sich für den Support an ix
I. Systemhinweise ..... **i**
1. Bootprozess, Init und Shutdown 1
1.1. Der Bootprozess 1
1.2. Der Bootprozess im Detail 1
1.3. Ausführen von zusätzlichen Programmen zum Zeitpunkt des Bootens 7
1.4. SysV Init Runlevels 7
1.5. Herunterfahren 9
2. Bootloader 11
2.1. Bootloader und Systemarchitektur 11
2.2. GRUB 11
2.3. Installation von GRUB 13
2.4. GRUB-Terminologie 13
2.5. GRUB-Oberflächen 15
2.6. GRUB-Befehle 16
2.7. Menükonfigurationsdatei von GRUB 18
2.8. LILO 19
2.9. Die LILO Konfigurationsdatei 21
2.10. Ändern von Runleveln zum Zeitpunkt des Bootens 22
2.11. Zusätzliche Ressourcen 23
3. Struktur des Dateisystems 25
3.1. Warum eine gemeinsame Struktur? 25
3.2. Übersicht über den Dateisystem-Hierarchiestandard (FHS) 25
3.3. Spezielle Dateispeicherstellen unter Red Hat Enterprise Linux 30
4. Das Verzeichnis `sysconfig` 31
4.1. Dateien im Verzeichnis `/etc/sysconfig/` 31
4.2. Verzeichnisse im Verzeichnis `/etc/sysconfig/` 43
4.3. Zusätzliche Ressourcen 44
5. Das `proc` Dateisystem 45
5.1. Ein virtuelles Dateisystem 45
5.2. Dateien im Hauptverzeichnis des `proc` Dateisystems 46
5.3. Verzeichnisse in `/proc/` 61
5.4. Benutzen von `sysctl` 78
5.5. Zusätzliche Ressourcen 78
6. Benutzer und Gruppen 81
6.1. Tools zum Management von Benutzern und Gruppen 81
6.2. Standardbenutzer 82
6.3. Standardgruppen 83
6.4. Benutzereigene Gruppen 85
6.5. Shadow-Utilities 86
6.6. Zusätzliche Informationsquellen 87
7. Das X Window System 89
7.1. XFree86 89

7.2. Desktop-Umgebungen und Window Manager ... 90
7.3. XFree86-Server-Konfigurationsdateien ... 91
7.4. Fonts ... 98
7.5. Runlevels und XFree86 ... 101
7.6. Zusätzliche Ressourcen ... 102
II. Hinweise für Netzwerk-Dienste ... 105
8. Netzwerk-Schnittstellen ... 107
8.1. Netzwerk-Konfigurationsdateien ... 107
8.2. Schnittstellen-Konfigurationsdateien ... 108
8.3. Schnittstellen-Kontrollskripts ... 115
8.4. Netzwerkfunktionsdateien ... 116
8.5. Zusätzliche Ressourcen ... 116
9. Netzwerk-Dateisystem (Network File System - NFS) ... 119
9.1. Wie es funktioniert ... 119
9.2. Starten und Anhalten von NFS ... 121
9.3. NFS-Server-Konfiguration ... 122
9.4. NFS-Client-Konfigurationsdateien ... 126
9.5. NFS Sichern ... 128
9.6. Zusätzliche Informationsquellen ... 129
10. Apache HTTP Server ... 131
10.1. Apache HTTP Server 2.0 ... 131
10.2. Migrieren von Apache HTTP Server 1.3 Konfigurationsdateien ... 133
10.3. Nach der Installation ... 143
10.4. Starten und Anhalten von `httpd` ... 143
10.5. Konfigurationsanweisungen in `httpd.conf` ... 144
10.6. Standard-Module ... 161
10.7. Hinzufügen von Modulen zu Ihrem Server ... 162
10.8. Virtuelle Hosts verwenden ... 163
10.9. Zusätzliche Ressourcen ... 165
11. Berkeley Internet Name Domain (BIND) ... 167
11.1. Einführung in den DNS ... 167
11.2. `/etc/named.conf` ... 169
11.3. Zone-Dateien ... 175
11.4. Die Verwendung von `rndc` ... 180
11.5. Erweiterte Funktionen von BIND ... 182
11.6. Allgemein zu vermeidende Fehler ... 184
11.7. Zusätzliche Ressourcen ... 184
12. Lightweight Directory Access Protocol (LDAP) ... 187
12.1. Warum LDAP? ... 187
12.2. LDAP Terminologie ... 188
12.3. OpenLDAP Daemons and Utilities ... 188
12.4. OpenLDAP Konfigurationsdateien ... 191
12.5. Das Verzeichnis `/etc/openldap/schema/` ... 191
12.6. Überblick über die OpenLDAP-Einrichtung ... 192
12.7. Konfigurieren Ihres Systems für die Authentifizierung mit OpenLDAP ... 194
12.8. Umwandeln von Verzeichnissen früherer Releases ... 195
12.9. Zusätzliche Ressourcen ... 196

III. Hinweis zur Sicherheit 199
13. Pluggable Authentication Modules (PAM) 201
13.1. Vorteile von PAM 201
13.2. PAM-Konfigurationsdateien 201
13.3. Format der PAM Konfigurationsdatei 201
13.4. Beispiele für PAM-Konfigurationsdateien 204
13.5. Module erstellen 206
13.6. PAM und Administrative-Credential-Caching 206
13.7. PAM und Besitzrechte von Geräten 208
13.8. Zusätzliche Ressourcen 209
14. TCP Wrappers und `xinetd` 211
14.1. TCP Wrappers 211
14.2. TCP Wrappers Konfigurationsdateien 212
14.3. `xinetd` 219
14.4. `xinetd`-Konfigurationsdateien 219
14.5. Zusätzliche Ressourcen 224
15. `iptables` 227
15.1. Paket-Filterung 227
15.2. Unterschiede zwischen `iptables` und `ipchains` 228
15.3. Mit `iptables`-Befehlen verwendete Optionen 229
15.4. `iptables`-Regeln werden gespeichert 236
15.5. `iptables` Kontrollskripte 237
15.6. `ip6tables` und IPv6 239
15.7. Zusätzliche Informationsquellen 239
16. Kerberos 241
16.1. Was ist Kerberos? 241
16.2. Kerberos-Terminologie 242
16.3. Funktionsweise von Kerberos 244
16.4. Kerberos und PAM 245
16.5. Konfigurieren eines Kerberos 5-Servers 246
16.6. Konfigurieren eines Kerberos 5-Clients 247
16.7. Zusätzliche Ressourcen 248
17. SSH-Protokoll 251
17.1. SSH-Merkmale 251
17.2. SSH Protokoll Versionen 252
17.3. Die Abfolge der Vorgänge einer SSH-Verbindung 252
17.4. OpenSSH-Konfigurationsdateien 254
17.5. Mehr als eine Secure Shell 256
17.6. Anfordern von SSH für Fernverbindungen 257
17.7. Zusätzliche Ressourcen 258
IV. Anhang 261
A. Allgemeine Parameter und Module 263
A.1. Spezifizieren der Modulparameter 263
A.2. SCSI-Parameter 263
A.3. Ethernet-Parameter 264
Stichwortverzeichnis 269
Colophon 283

Einführung

Willkommen im *Red Hat Enterprise Linux Referenzhandbuch*.

Das *Red Hat Enterprise Linux Referenzhandbuch* enthält nützliche Informationen über Ihr Red Hat Enterprise Linux-System. Der Inhalt reicht von grundlegenden Konzepten, wie z.B. Struktur des Dateisystems, bis hin zu den Details, wie z.B. Systemsicherheit und Authentifizierungskontrolle. Wir hoffen, dass dieses Buch zu einem wertvollen Nachschlagewerk für Sie wird.

Wenn Sie ein wenig mehr über die Funktionsweise des Red Hat Enterprise Linux-Systems erfahren möchten, ist dieser Leitfaden genau das Richtige. Es werden unter anderem folgende Themen behandelt:

- Boot-Prozess
- Struktur des Dateisystems
- Das X Window System
- Netzwerkleistungen
- Sicherheits-Tools

1. Änderungen an diesem Handbuch

Dieses Handbuch wurde zur besseren Übersicht neu angeordnet und mit den neuesten Eigenschaften von Red Hat Enterprise Linux 3 aktualisiert. Zu den Änderungen gehören u.a.:

Ein neues FTP Kapitel

Das neue *FTP* Kapitel erklärt das FTP-Protokoll und stellt eine detaillierte Liste an Konfigurationsoptionen für den Standard- FTP-Server bereit: `vsftpd`.

Ein aktualisiertes Netzwerk-Dateisysteme (NFS) Kapitel

Das *Netzwerk-Dateisystem (NFS)* wurde komplett überarbeitet und für eine bessere Klarheit neu organisiert. Außerdem wurden neue Bereiche hinzugefügt, z.B. TCP und Kontrolllisten-Unterstützung.

Ein aktualisierter ModuleAnhang

Der *Module*-Anhang ist komplett überarbeitet worden. Es wurden Anweisungen für das `bonding` Modul hinzugefügt, das Benutzern erlaubt, mehrfache Netzwerk-Schnittstellenkarten zusammenzubinden, als ob sie eine wären.

Das Kapitel Netzwerkschnittstellen wurde aktualisiert.

Das Kapitel *Netzwerkschnittstellen* wurde aktualisiert und enthält jetzt IPSec und bindende Schnittstellen.

Das Kapitel Apache HTTP Server wurde aktualisiert.

Es steht nun ein Leitfaden zur Migration von Version 1.3 nach Version 2.0 von Apache HTTP Server zur Verfügung. Außerdem wurde die Liste der Serverkonfigurations-Optionen auf den neuesten Stand gebracht. Ein besonderer Dank geht an **Gary Benson** und **Joe Orton** für ihre harte Arbeit am Apache HTTP Server-Migrationsleitfaden.

Ein aktualisiertes Das X Window System Kapitel

Das X Window System wurde komplett umgeschrieben und für eine bessere Klarheit neu organisiert. Weiterhin wurden Anleitungen zur Font-Konfiguration hinzugefügt.

Das Kapitel Benutzer und Gruppen wurde aktualisiert.

Das Kapitel *Benutzer und Gruppen* wurde aktualisiert.

Bevor Sie dieses Handbuch lesen, sollten Sie den Inhalt des *Red Hat Enterprise Linux Installationshandbuch* über Installationsfragen, des *Red Hat Enterprise Linux Introduction to System Administration* über grundlegende Verwaltungskonzepte, des*Red Hat Enterprise Linux Handbuch zur System-Administration* für allgemeine Anweisungen zur benutzerdefinierten Einstellung sowie des *Red Hat Enterprise Linux Sicherheitshandbuch* für Anweisungen im Zusammenhan mit Sicherheit kennen.Das *Red Hat Enterprise Linux Referenzhandbuch* enthält Informationen zu fortgeschrittenen Themen.

HTML-, PDF- und RPM-Versionen der Handbücher sind auf der Red Hat Enterprise Linux Dokumentations-CD und Online unter http://www.redhat.com/docs/ erhältlich.

Anmerkung

Obwohl dieses Handbuch die neuesten Informationen enthält, lesen Sie die *Red Hat Enterprise Linux Release-Notes* für weitere Information, die zum Druck dieses Handbuchs noch nicht vorlagen. Diese können auf der Red Hat Enterprise Linux CD #1 und Online unter http://www.redhat.com/docs/ gefunden werden.

2. So finden Sie die geeignete Dokumentation

Es ist wichtig, dass Sie sich jene Informationen beschaffen, die für Ihren Kenntnisstand in Sachen Linux geeignet ist. Andernfalls könnten Sie sich schnell überfordert fühlen oder nicht an die Informationen gelangen, mit deren Hilfe Sie Probleme lösen können. Das *Red Hat Enterprise Linux Referenzhandbuch* beschäftigt sich mit den eher technischen Aspekten und Optionen eines Red Hat Enterprise Linux-Systems. Dieser Abschnitt wird Ihnen dabei helfen, zu entscheiden, ob Sie dieses Handbuch als Informationsquelle benutzen wollen, oder ob Sie andere Red Hat Enterprise Linux Handbücher, einschließlich der Online-Quellen, bei Ihrer Suche zu Rate ziehen wollen.

Es gibt drei verschiedene Kategorien von Red Hat Enterprise Linux-Benutzern. Und jede dieser Kategorien benötigt andere Dokumentations- und Informationsquellen. Um genauer beurteilen zu können, welche für Sie am besten ist, sollten Sie sich klar darüber werden, wie umfangreich Ihre Vorkenntnisse sind:

Linux-Einsteiger

Dieser Benutzertyp hat bislang noch kein Linux- oder Linux-ähnliches Betriebssystem verwendet oder verfügt über nur geringe Kenntnisse in Linux. Möglicherweise sind bereits gewisse Kenntnisse im Umgang mit anderen Betriebssystemen vorhanden (beispielsweise Windows) Trifft dies auf Sie zu? Falls ja, sollten Sie sich Abschnitt 2.1 durchlesen.

Bereits einige Erfahrungen mit Linux

Dieser Benutzertyp hat Linux (aber nicht Red Hat Enterprise Linux) zuvor bereits erfolgreich installiert und verwendet. Er verfügt unter Umständen auch über vergleichbare Erfahrungen mit anderen Betriebssystemen, die Linux ähneln. Trifft das auf Sie zu? Falls ja, sollten Sie sich Abschnitt 2.2 durchlesen.

Erfahrener Benutzer

Dieser Benutzertyp hat Red Hat Enterprise Linux bereits zuvor erfolgreich installiert und verwendet. Haben Sie gute Erfahrung in Sachen Linux? Falls ja, lesen Sie Abschnitt 2.3

2.1. Dokumentation für Linux-Einsteiger

Ein Linux-Einsteiger könnte von den vielen Informationen, die über jedes Argument, wie z.B. Drucken und Starten, zur Verfügung stehen, überfordert sein. Bevor Sie sich mit diesen Fortgeschrittenen-Themen auseinandersetzen, ist es sicher eine gute Idee, einen Schritt zurückzugehen, um zunächst einmal genügend Informationen über die Funktionsweise von Linux zu sammeln.

Ihr erstes Ziel sollte es zunächst sein, sich die notwendige Dokumentation zu beschaffen. Die Wichtigkeit dieses Schritts kann gar nicht oft genug betont werden. Ohne die erforderlichen Informationen können Sie Ihr Red Hat Enterprise Linux-System nämlich nicht nach Ihren Wünschen einrichten, und das kann zu Frustration führen.

Sie sollten sich die folgende Linux-Dokumentation beschaffen:

- *Ein kurzer Überblick über die Geschichte von Linux* — Viele Aspekte von Linux lassen sich durch die historische Entwicklung dieses Betriebssystems besser verstehen. Es gibt sogar so etwas wie eine "Linux-Kultur", die wiederum eng mit dieser Geschichte und den Ansprüchen und Erfordernissen der Vergangenheit zusammenhängt. Wenn Sie sich zumindest ein bisschen mit der Entstehungsgeschichte von Linux auskennen, werden Sie im voraus herausfinden, wie Sie viele Ihrer potentiellen Probleme lösen können, bevor sie überhaupt auftreten.
- *Eine Erklärung der Funktionsweise von Linux* — Auch wenn es sicherlich nicht nötig ist, sich mit den exotischsten Fragestellungen hinsichtlich des Linux-Kernels auseinanderzusetzen, ist doch ein grundlegendes Verständnis der Funktionsweise von Linux sehr hilfreich. Diese Kenntnisse sind vor allem dann wichtig, wenn Sie sich bereits mit anderen Betriebssystemen auskennen. Einige der Konzepte dieser Betriebssysteme können möglicherweise nicht direkt auf Linux übertragen werden.
- *Eine einführende Befehlsübersicht (mit Beispielen)* — Dies ist unter Umständen der wichtigste Punkt bei Ihrer Suche nach einer geeigneten Linux-Dokumentation. Die grundlegende Philosophie von Linux lautet, dass es besser ist, viele kleine, miteinander verschiedenartig verbundene Befehle zu verwenden, als wenige große (und sehr komplizierte) Befehle zu haben, die die ganze Angelegenheit alleine erledigen. Ohne Beispiele für diesen von Linux vertretenen Ansatz für das Erledigen von Aufgaben könnte es sein, dass Sie sich von der Vielzahl der Befehle überwältigt sehen, die auf dem Red Hat Enterprise Linux-System zur Verfügung stehen.

  Denken Sie aber bitte immer daran, dass Sie sich nicht an alle Ihnen zur Verfügung stehenden Linux-Befehle erinnern müssen! Es gibt verschiedene Techniken und Hilfestellungen, um herauszufinden, welche Art Befehl Sie brauchen, um eine Aufgabe zu erledigen. Sie sollten also lediglich grob darüber Bescheid wissen, wie Linux funktioniert, was Sie erreichen wollen und und wie Sie den Zugang zu dem Tool finden, das Ihnen dann genaue Anweisungen dazu gibt, wie Sie den Befehl ausführen müssen.

Das *Red Hat Enterprise Linux Installationshandbuch* ist eine hervorragende Informationsquelle,die Ihnen dabei hilft, Ihr Red Hat Enterprise Linux-System erfolgreich zu installieren und grundlegend zu konfigurieren. Das *Red Hat Enterprise Linux Introduction to System Administration* ist ein exzellenter Ausgangspunkt, wenn Sie die Grundlagen der Systemverwaltung lernen wollen. Sie sollten mit diesen zwei Büchern beginnen und sich so ein Basiswissen über Red Hat Enterprise Linux aneignen. Es wird nicht lange dauern, dass Ihnen auch kompliziertere Konzepte sinnvoll erscheinen, weil Sie die Grundgedanken dahinter bereits verstanden haben.

Außer den Red Hat Enterprise Linux-Handbüchern stehen Ihnen noch viele andere hervorragende Dokumentationsquellen zur Verfügung, die - sofern sie nicht gratis sind - auch nicht viel kosten:

2.1.1. Einführung in Linux Webseiten

- http://www.redhat.com — Auf der Red Hat Website finden Sie Links zum Linux Documentation Project (LDP), zu den Online-Versionen der Red Hat Enterprise Linux-Handbücher, den FAQs

(häufig gestellte Fragen), zu der Datenbank für die Suche nach einer Linux-Benutzergruppe in Ihrer Nähe, zu technischen Informationen in der Red Hat Support- Knowledge-Base (eine weitere Datenbank zur Unterstützung) und vieles mehr.

- http://www.linuxheadquarters.com — Auf der Linux Headquarters-Website finden Sie leicht verständliche schrittweise Anweisungen zu einer Vielzahl von Linux-Aufgaben.

2.1.2. Einführung in die Linux Newsgroups

Sie können an den Newsgroups teilnehmen, indem Sie den Diskussionen anderer Benutzer folgen, die versuchen, Probleme zu lösen, oder indem Sie selbst aktiv Fragen stellen oder beantworten. Erfahrene Linux-Benutzer sind dafür bekannt, dass Sie Einsteigern gerne bei Ihren unterschiedlichen Fragen zu Linux unter die Arme greifen — vor allem, wenn Sie Ihre Fragen vor dem richtigem Publikum stellen. Sollten Sie allerdings keinen Zugang zu einer der News Reader-Anwendungen haben, können Sie unter der folgenden Webadresse nach entsprechenden Informationen hierzu suchen: http://groups.google.com/. Es gibt nämliche Dutzende Linux-relevante Newsgroups, unter anderem die folgenden:

- linux.help — Eine hervorragende Adresse, sich von Linux-Kollegen helfen zu lassen.
- linux.redhat — In dieser Newsgroup geht es hauptsächlich um Red Hat Enterprise Linux-spezifische Themen.
- linux.redhat.install — Dieser Newsgroup können Sie Fragen zur Installation stellen oder nachschauen, wie andere Benutzer ähnliche Probleme lösen oder gelöst haben.
- linux.redhat.misc — Fragen bzw. Anfragen, die nicht unbedingt in die gängigen Kategorien gehören, sollten Sie hier stellen.
- linux.redhat.rpm — Eine gute Adresse, die Sie aufsuchen sollten, wenn Sie Schwierigkeiten haben, mit RPMbestimmte Ziele zu erreichen.

2.1.3. Linux-Bücher für Anfänger

- *Red Hat Linux for Dummies, 2. Auflage* von Jon "maddog" Hall; IDG
- *Special Edition Using Red Hat Linux* von Alan Simpson, John Ray und Neal Jamison; Que
- *Running Linux* von Matt Welsh und Lar Kaufman; O'Reilly & Associates
- *Red Hat Linux 9 Unleashed* von Bill Ball und Hoyle Duff; Pearson Education

Die hier vorgeschlagenen Bücher sind ausgezeichnete Informationsquellen für die allgemeinen Grundkenntnisse über das Red Hat Enterprise Linux- System. Detailliertere Informationen über die in diesem Handbuch beprochenen Themen finden Sie in bestimmten Fachbüchern, deren Titel in vielen Kapiteln dieses Handbuches für Sie aufgelistet wurden - meist im *Weitere Informationsquellen*-Bereich.

Eine hervorragende Informationsquelle für angehende Systemadministratoren ist *Red Hat Enterprise Linux Introduction to System Administration*. Dieses Buch wurde geschrieben, um Strategien zur Administration von Red Hat Enterprise Linux zu erklären. Ein wirklich geeigneter Ausgangspunkt für jene, die die Grundlagen der Systemadministration lernen wollen.

2.2. Für erfahrene Linux-Benutzer

Wenn Sie bereits andere Linux-Produkte verwendet haben, sind Ihnen vermutlich die am gängigsten Befehle längst geläufig. Möglicherweise haben Sie ein eigenes Linux-System installiert und sogar

Software aus dem Internet heruntergeladen und installiert. Nach der Installation von Linux können Konfigurationsfragen allerdings auch für Sie sehr verwirrend sein.

Das *Red Hat Enterprise Linux Handbuch zur System-Administration* wird Ihnen die verschiedenen Optionen erläutern, mit denen Sie Ihr Red Hat Enterprise Linux-System konfigurieren und gewisse Ziele erreichen können. Nutzen Sie dieses Handbuch dazu, sich mit bestimmten Konfigurationsoptionen und ihrer Umsetzung vertraut zu machen.

Wenn Sie Software installieren, die nicht im *Red Hat Enterprise Linux Handbuch zur System-Administration* enthalten ist, hilft es oft, sich anzusehen, wie andere Benutzer unter ähnlichen Voraussetzungen vorgegangen sind. Die HOWTO-Dokumente des Linux Documentation Project stehen Ihnen unter http://www.redhat.com/mirrors/LDP/HOWTO/HOWTO-INDEX/howtos.html zur Verfügung und dokumentieren ganz bestimmte Linux-Aspekte - von der esoterischen Veränderung des Low-Level-Kernels bis hin zum Einsatz von Linux für einen Amateur-Radiosender.

Wenn Sie sich mit Sicherheitsfragen auseinandersetzen wollen, ist das *Red Hat Enterprise Linux Sicherheitshandbuch* eine großartige Informationsquelle —. Hier werden die besten Strategien und Praktiken zu Sicherung von Red Hat Enterprise Linux in knapper Weise erklärt.

2.3. Dokumentation für Linux-Gurus

Wenn Sie Red Hat Enterprise Linux bereits seit langem benutzen, wissen Sie wahrscheinlich längst, dass der beste Weg zum Verständnis eines spezifischen Programms das Lesen seines Quellcodes und/oder der Konfigurationsdateien ist. Ein großer Vorteil von Red Hat Enterprise Linux ist, dass der Quellcode von allen Benutzern gelesen werden kann.

Natürlich ist nicht jeder ein Programmierer, und Sie können mit dem Quellcode daher vielleicht wenig anfangen. Wenn Sie jedoch nur ein wenig Erfahrungen und Kenntnisse haben und wissen, wie man ihn lesen kann, finden Sie im Quellcode die Antwort auf alle Ihre Fragen.

3. Dokumentkonventionen

Beim Lesen dieses Handbuchs werden Sie feststellen, dass bestimmte Wörter in verschiedenen Fonts, Schriftbildern, Größen usw. dargestellt sind. Diese Unterscheidung folgt einer bestimmten Ordnung: bestimmte Wörter werden auf die gleiche Weise dargestellt, um darauf hinzuweisen, dass sie zu einer bestimmten Kategorie gehören. Typen von Wörtern, die so dargestellt werden, schließen Folgende ein:

`Befehl`

Linux-Befehle (sowie Befehle anderer Betriebssysteme, sofern verwendet) werden auf diese Weise dargestellt. Diese Darstellungsart weist darauf hin, dass Sie das Wort oder den Satz in die Befehlszeile eingeben und die [Enter-Taste] drücken können, um den entsprechenden Befehl auszuführen. Gelegentlich enthält ein Befehl Wörter, die eigentlich auf eine andere Weise dargestellt werden würden (beispielsweise Dateinamen). In einem solchen Fall werden sie als Teil des Befehls betrachtet, und der gesamte Satz wird als Befehl dargestellt. Beispiel:

Verwenden Sie den Befehl `cat testfile`, um den Inhalt einer Datei mit dem Namen `testfile` in einem aktuellen Verzeichnis anzeigen zu lassen.

`Dateiname`

Datei- und Verzeichnisnamen sowie die Namen von Pfaden und RPM-Paketen werden auf diese Weise dargestellt, was bedeutet, dass eine bestimmte Datei oder ein bestimmtes Verzeichnis mit diesem Namen in Ihrem System vorhanden ist. Beispiele:

Die Datei `.bashrc` in Ihrem Home-Verzeichnis enthält Bash-Shell Definitionen und Aliase für Ihren Gebrauch.

Die Datei `/etc/fstab` enthält Informationen über verschiedene Systemgeräte und Dateisysteme.

Installieren Sie den `webalizer` RPM, wenn Sie ein Analyseprogramm für eine Webserver-Protokolldatei verwenden möchten.

Applikation

Diese Darstellungsart weist darauf hin, dass es sich bei diesem Programm um eine Endbenutzer-Anwendung handelt (im Gegensatz zur System-Software). Beispiel:

Verwenden Sie **Mozilla**, um im Web zu browsen.

[Taste]

Die Tasten der Tastatur werden auf diese Weise dargestellt. Beispiel:

Um die [Tab]-Vervollständigung zu verwenden, geben Sie einen Buchstaben ein und drücken Sie anschließend die Taste [Tab]. Auf diese Weise wird die Liste der Dateien im Verzeichnis angezeigt, die mit diesem Buchstaben beginnen.

[Tasten]-[Kombination]

Eine Tastenkombination wird auf diese Art und Weise dargestellt.

Mit der Tastenkombination [Strg]-[Alt]-[Rücktaste] beenden Sie Ihre grafische Sitzung und kehren zum grafischen Anmeldebildschirm oder zur Konsole zurück.

Text in der GUI-Schnittstelle

Überschriften, Worte oder Sätze, die Sie auf dem GUI-Schnittstellenbildschirm oder in Window finden, werden in diesem Stil wiedergegeben. Wenn Sie daher einen Text in diesem Stil finden, soll dieser einen bestimmten GUI-Bildschirm oder ein Element eines GUI-Bildschirms (z.B. ein Text, der sich auf ein Kontrollkästchen oder auf ein Feld bezieht) identifizieren. Beispiel:

Wählen Sie das Kontrollkästchen **Passwort erforderlich**, wenn Ihr Bildschirmschoner passwortgeschützt sein soll.

Erste Menüstufe auf einem GUI-Bildschirm oder in einem Fenster

Wenn ein Wort auf diese Art und Weise dargestellt ist, zeigt dies an, dass es sich hierbei um den Anfang eines Pulldown-Menüs handelt. Beim Klicken auf das Wort auf dem GUI-Bildschirm erscheint der Rest des Menüs. Zum Beispiel:

Unter **Datei** auf dem GNOME-Terminal sehen Sie die Option **Neuer Tab**, mit dem Sie mehrere Shell Prompts im gleichen Fenster öffnen können.

Wenn Sie eine Befehlsreihe aus einem GUI-Menü eingeben wollen, wird diese entsprechend dem folgenden Beispiel angezeigt:

Indem Sie **Hauptmenü** (im Panel) => **Programmieren** => **Emacs** wählen, starten Sie den Texteditor **Emacs**.

Schaltfläche auf einem GUI-Bildschirm oder in einem Fenster

Diese Darstellungsweise zeigt an, dass man den betreffenden Text auf der Schaltfläche eines GUI-Bildschirms finden kann. Zum Beispiel:

Indem Sie auf die Schaltfläche **Zurück** klicken, kehren Sie auf die Website zurück, die Sie zuletzt angesehen haben.

`Computerausgabe`

Text, der in diesem Stil dargestellt wird, ist Text, der in einem Shell-Prompt ausgegeben wird, wie Fehlermeldungen und Antworten auf bestimmte Befehle. Zum Beispiel:

Durch Eingabe von `ls` erscheint der Inhalt eines Verzeichnisses. Zum Beispiel:

```
Desktop                about.html       logs          paulwesterberg.png
Mail                   backupfiles      mail          reports
```

Die Ausgabe, die als Antwort auf den Befehl erscheint (in diesem Fall der Inhalt des Verzeichnisses), wird auf diese Art und Weise dargestellt.

`Prompt`

Ein Prompt wird auf diese Art und Weise dargestellt, wenn der Computer Ihnen mitteilen will, dass Sie nun eine Eingabe tätigen können. Beispiele:

```
$
```

```
#
```

```
[stephen@maturin stephen]$
```

```
leopard login:
```

`Benutzereingabe`

Ein Text wird auf diese Art und Weise dargestellt, wenn er vom Benutzer entweder in die Befehlszeile oder in die Textbox auf einem GUI-Bildschirm eingegeben werden soll. Im folgenden Beispiel wird **`text`** in diesem Stil angezeigt:

Mit dem Befehl **`text`** am Prompt `boot:` booten Sie Ihr System in das textbasierte Installationsprogramm.

`replaceable`

Text, der vom Benutzer ersetzt werden soll, wird in diesem Stil dargestellt. Im folgenden Beispiel ist *<version-number>* in dieser Form dargestellt.

Das Verzeichnis für den Kernel-Source ist `/usr/src/`*<version-number>*`/`, wobei *<version-number>* die Version des installierten Kernel ist.

Weiterhin machen wir Sie mit Hilfe von bestimmten Strategien auf bestimmte Informationen aufmerksam. Entsprechend dem Wichtigkeitsgrad, das die jeweilige Information für Ihr System hat, sind diese Items entweder als Anmerkung, Hinweis oder Warnung gekennzeichnet. Zum Beispiel:

Anmerkung

Beachten Sie, dass Linux ein fallspezifisches System ist. In anderen Worten bedeutet dies, dass Rose nicht das gleiche ist wie ROSE und dies auch nicht das gleiche wie rOsE.

Tipp

Das Verzeichnis `/usr/share/doc/` enthält zusätzliche Dokumentationen für im System installierte Pakete.

Wichtig

Wenn Sie die DHCP Konfigurationsdatei bearbeiten, werden die Änderungen erst wirksam, wenn Sie den DHCP-Daemon neu gestartet haben.

Achtung

Führen Sie keine alltäglichen Aufgaben als root aus — verwenden Sie hierzu außer für den Fall, dass Sie einen root-Account für Ihre Systemverwaltung benutzen, einen regulären Benutzeraccount.

Warnung

Seien Sie vorsichtig und entfernen Sie lediglich die notwendigen Red Hat Enterprise Linux Partitionen. Das Entfernen anderer Partitionen könnte zu Datenverlusten oder zur Korruption der Systemumgebung führen.

4. Verwenden der Maus

Für die Benutzung von Red Hat Enterprise Linux ist eine Maus mit drei Tasten vorgesehen. Falls Sie im Besitz einer Maus mit nur zwei Tasten sind, sollten Sie während des Installationsprozesses die Drei-Tasten-Emulation wählen. Mit der Drei-Tasten-Emulation betätigen Sie die dritte, nicht real vorhandene (mittlere) Maus-Taste, indem Sie die beiden vorhandenen Tasten gleichzeitig drücken.

Immer wenn Sie in diesem Dokument dazu aufgefordert werden, etwas mit der Maus anzuklicken, bedeutet dies automatisch, dass Sie mit der linken Taste klicken sollen. Falls Sie hingegen die mittlere oder die rechte Maus-Taste betätigen sollen, werden Sie ausdrücklich dazu aufgefordert. (Rechts und links sind genau umgekehrt, wenn Sie Ihre Maus für die Benutzung durch einen Linkshänder konfiguriert haben.)

Wahrscheinlich kennen Sie den Ausdruck "ziehen und ablegen" (Drag & Drop) bereits. Wenn Sie dazu aufgefordert werden, eine Item auf Ihrem GUI-Desktop zu ziehen und abzulegen, bedeutet dies, dass Sie etwas anklicken sollen und dann die Maus-Taste gedrückt halten. Sie halten nun die Maus-Taste weiterhin gedrückt und ziehen das Element, indem Sie die Maus auf die gewünschte Position bewegen. Nachdem Sie auf dieser Position angekommen sind, lassen Sie die Maus-Taste los und legen damit das Element ab.

5. Kopieren und Einfügen von Text mit X

Das Kopieren und Einfügen von Text mit der Maus und dem X Window System ist sehr einfach. Um Text zu kopieren, klicken Sie auf Ihre linke Maustaste und ziehen Sie den Cursor über den Text, um ihn hervorzuheben. Um den Text an einer anderen Stelle einzufügen, klicken Sie einfach an der gewünschten Stelle auf die mittlere Maustaste.

6. Fortsetzung folgt!

Das *Red Hat Enterprise Linux Referenzhandbuch* ist Teil der Verpflichtungvon Red Hat, die Red Hat Enterprise Linux-Benutzer durch zeitgerechte und nützliche Informationen zu unterstützen. Die zukünftigen Ausgaben werden erweiterte Informationen über Änderungen im Systemaufbau und in der Systemorganisation, neue und leistungsstarke Sicherheits-Tools und weitere Ressourcen enthalten, mit denen Sie die Leistungsfähigkeit Ihres Red Hat Enterprise Linux-Systems — und Ihre eigenen Fähigkeiten noch weiter steigern können.

Hier könnten wir Ihre Hilfe gebrauchen!

6.1. Wir brauchen Ihre Rückmeldung!

Wenn Sie Fehler im *Red Hat Enterprise Linux Referenzhandbuch* entdecken oder Vorschläge bzw. Anregungen zur Verbesserung dieses Handbuchs machen wollen, würden wir uns sehr freuen, von Ihnen zu hören! Schreiben Sie bitte an Bugzilla (http://bugzilla.redhat.com/bugzilla) mit dem Kennwort *rhel-rg*.

Geben Sie bitte dabei auch die Kennziffer dieses Handbuchs ein:

```
rhel-rg(DE)-3-Print-RHI (2003-07-25T17:13)
```

Geben Sie bitte auch die Kennziffer des Handbuchs an, damit wir wissen, um welche Version Ihnen vorliegt.

Wenn Sie Vorschläge zur Verbesserung der Dokumentation haben, beschreiben Sie uns Ihren Vorschlag bitte so präzise wie möglich. Und wenn Sie einen Fehler entdeckt haben, hilft es uns , wenn Sie uns den genauen Abschnitt und die Textstelle angeben - nur so können wir die Stelle finden und korrigieren.

7. Melden Sie sich für den Support an

Wenn Sie eine offizielle Version von Red Hat Enterprise Linux 3 erworben haben, können Sie die Vorteile als Kunde von Red Hat nutzen.

Sie können einige oder andere der folgenden Vorteile nutzen, je nachdem welches Produkt Sie erworben haben:

- Red Hat Support — Sie erhalten vom Red Hat, Inc. Support-Team Hilfe bei der Installation.
- Red Hat Network — Einfaches Update Ihrer Pakete. Sie erhalten auf Ihr System abgestimmte Sicherheits-Meldungen. Unter http://rhn.redhat.com/ finden Sie weitere Details.
- *Under the Brim: The Official Red Hat E-Newsletter* — Sie erhalten monatlich die neuesten Mitteilungen und Produktinformationen direkt von Red Hat.

Melden Sie sich unter http://www.redhat.com/apps/activate/. Ihre Produkt ID finden Sie auf der schwarz/rot/weißen Karte in Ihrer Red Hat Enterprise Linux Box.

Weitere Informationen über den technischen Support für Red Hat Enterprise Linux finden Sie im Anhang *Technischen Support anfordern* im *Red Hat Enterprise Linux Installationshandbuch*.

Viel Glück und vielen Dank, dass Sie sich für Red Hat Enterprise Linux entschieden haben!

Das Red Hat Dokumentationsteam

I. Systemhinweise

Um das System wirkungsvoll zu leiten, ist es wichtig, seine Komponenten zu kennen und zu wissen, wie sie zusammenarbeiten. Dieser Abschnitt geht auf viele verschiedene Aspekte des Sytems ein. Behandelt werden der Boot-Prozess, die grundlegende Anordnung des Dateisystems, der Ort von bedeutenden Systemdateien und Systemverzeichnissen und das Grundkonzept von Benutzern und Benutzergruppen. Zusätzlich wird das Window X System genau erklärt.

Inhaltsverzeichnis

1. Bootprozess, Init und Shutdown **1**
2. Bootloader **11**
3. Struktur des Dateisystems **25**
4. Das Verzeichnis `sysconfig` **31**
5. Das `proc` Dateisystem **45**
6. Benutzer und Gruppen **81**
7. Das X Window System **89**

redhat

Kapitel 1.

Bootprozess, Init und Shutdown

Einer der größten Vorteile von Red Hat Enterprise Linux ist die flexible und Benutzer-konfigurierbare Methode des Bootens und Herunterfahrens des Betriebssystems. Benutzer können viele Aspekte des Bootvorgangs frei einstellen, einschließlich welche Programme während des Bootens gestartet werden. Ebenso beendet das richtige Herunterfahren des Systems die Prozesse auf organisierte und konfigurierbare Art und Weise, auch wenn die individuelle Gestaltung dieses Prozesses kaum erforderlich ist.

Das Verstehen der Funktionsweise der Boot- und Shutdownprozesse erleichtert nicht nur das individuelle Gestalten je nach Ihren Anforderungen, sondern macht auch das Beheben von Fehlern einfacher, die beim Starten oder Herunterfahren des Systems auftreten können.

1.1. Der Bootprozess

Nachfolgend werden die grundlegenden Phasen des Bootprozesses für ein x86-System beschrieben:

1. Das System-BIOS prüft das System und startet den ersten Bootloader auf dem MBR der primären Festplatte.
2. Der Bootloader der ersten Phase wird in den Arbeitsspeicher geladen und startet den Bootloader der zweiten Phase von der `/boot/`-Partition.
3. Der Bootloader der zweiten Phase lädt den Kernel in den Arbeitsspeicher, welcher wiederum seinerseits alle erforderlichen Module lädt und die root-Partition als schreibgeschützt mountet.
4. Der Kernel übergibt die Steuerung des Bootprozesses an das Programm `/sbin/init`.
5. Das Programm `/sbin/init` lädt alle Dienste und Tools des Arbeitsplatzes und mountet alle in `/etc/fstab` genannten Partitionen.
6. Dem Benutzer wird eine Anmeldeaufforderung für das gerade gestartete Linux-System angezeigt.

Da das Konfigurieren des Bootprozesses häufiger ist als die individuelle Gestaltung des Herunterfahrens, wird im restlichen Kapitel die Funktionsweise des Bootprozesses sowie die individuelle Anpassung an Ihre Bedürfnisse detailliert behandelt.

1.2. Der Bootprozess im Detail

Der wirkliche Beginn des Bootprozesses hängt von der verwendeten Hardware-Plattform ab. Sobald jedoch der Kernel vom System gefunden und geladen wurde, ist der standardmäßige Bootprozess auf allen Architekturen identisch. Dieses Kapitel bezieht sich auf eine x86-Architektur.

1.2.1. Das BIOS

Wenn ein x86-Computer gestartet wird, sucht der Prozessor am Ende des Systemspeichers nach dem *Basic Input/Output System* oder *BIOS*-Programm und führt es aus. Das BIOS steuert nicht nur den ersten Schritt des Bootprozesses, sondern stellt auch die Schnittstelle der untersten Ebene zu den Peripheriegeräten dar. Daher ist es im schreibgeschützten permanenten Speicher abgelegt und ständig einsatzbereit.

Andere Plattformen verwenden verschiedene Programme, um Aufgaben der niedrigen Ebene durchzuführen, die denen des BIOS auf einem x86-System stark ähneln. Itanium-basierte Computer zum Bei-

spiel verwenden die *Extensible Firmware Interface* (*EFI*)-*Shell*, während Alpha-Systeme die *SRM-Konsole* verwenden.

Nach dem Start prüft das BIOS das System, sucht und prüft Peripheriegeräte und sucht dann nach einem gültigen Gerät zum Starten des Systems. Normalerweise prüft es zuerst die Disketten- und CD-ROM-Laufwerke auf startfähige Medien und sucht dann auf den Festplatten des Systems. Die Reihenfolge der zum Booten durchsuchten Laufwerke wird oft durch eine Einstellung auf dem BIOS gesteuert. Häufig ist die erste, zum Booten festgelegte Festplatte das Laufwerk C oder das Master-IDE-Gerät auf dem primären IDE-Bus. Das BIOS lädt das Programm, das im ersten Sektor dieses Geräts gespeichert ist und *Master Boot Record* oder *MBR* genannt wird, in den Speicher. Der MBR ist nur 512 Bytes groß und enthält vom Rechner lesbare Anweisungen zum Booten des Rechners zusammen mit der Partitionstabelle. Nach dem Laden prüft das BIOS das jeweilige Programm auf dem MBR.

1.2.2. Der Bootloader

In diesem Abschnitt werden die Bootloader für die x86-Plattform betrachtet. Je nach Systemarchitektur kann der Bootprozess leicht variieren. Unter Abschnitt 1.2.2.1 finden Sie einen kurzen Überblick zu nicht-x86 Bootloadern.

Unter Red Hat Enterprise Linux stehen zwei Bootloader zur Verfügung: *GRUB* oder *LILO*. GRUB ist der Default-Bootloader, LILO ist allerdings verfügbar für alle die diesen entweder benötigen oder vorziehen. Für weitere Informationen zum Konfigurieren von GRUB oder LILO, siehe Kapitel 2.

Die Linux-Bootloader für x86-Plattformen werden in mindestens zwei Phasen unterteilt. Die erste Phase ist ein kleiner binärer Rechnercode auf dem MBR. Seine einzige Aufgabe besteht im Suchen des Bootloaders der zweiten Phase und dem Laden des ersten Teils in den Arbeitsspeicher.

GRUB ist der neuere Bootloader und hat den Vorteil, dass er ext2 und ext3 [1] Partitionen lesen kann und seine Konfigurationsdatei — `/boot/grub/grub.conf` — zur Bootzeit laden kann. Sehen Sie Abschnitt 2.7 für Informationen zum Bearbeiten dieser Datei.

Unter LILO verwendet der Bootloader der 2. Phase die Informationen auf dem MBR, um zu ermitteln, welche Bootoptionen dem Benutzer zur Verfügung stehen. Dies bedeutet, dass Sie bei jeder Konfigurationsänderung oder manuellen Kernelaktualisierung den Befehl `/sbin/lilo -v -v` ausführen müssen, um die entsprechenden Informationen auf den MBR zu schreiben. Detaillierte Informationen hierzu finden Sie unter Abschnitt 2.8.

Tipp

Wenn Sie ein Upgrade des Kernel mit Hilfe des **Red Hat Update Agent** durchführen, wird die Konfigurationsdatei des Bootloader automatisch aktualisiert. Weitere Informationen zu RHN finden Sie unter folgendem URL: https://rhn.redhat.com

Wenn der Bootloader der 2. Phase in den Arbeitsspeicher geladen ist, wird dem Benutzer der grafische Anfangsbildschirm mit den verschiedenen Betriebssystemen oder Kernels angezeigt, die gestartet werden sollen. Auf diesem Bildschirm kann ein Benutzer die Pfeiltasten benutzen, um ein Betriebssystem auszuwählen und dann die [Enter-Taste] drücken, um dieses zu booten. Sollte keine Taste gedrückt werden, wird der Bootloader nach einiger Zeit das standardmäßig ausgewählte Betriebsystem booten.

1. GRUB liest ext3 Dateisysteme als ext2, unabhängig von der Journal-Datei. Sehen Sie das Kapitel *Das ext3 Dateisystem* im *Red Hat Enterprise Linux Handbuch zur System-Administration* für mehr Informationen zum ext3 Dateisystem.

Anmerkung

Wenn SMP-Kernel-Support (Symmetric Multi-Processor) installiert ist, stehen Ihnen beim Erststart des Systems mehrere Optionen zur Verfügung. Unter LILO wird `linux`, für den SMP Kernel, und `linux-up`, für den Einzelprozessor, angezeigt. Unter GRUB wird `Red Hat Enterprise Linux (<Kernelversion>-smp)`, für den SMP Kernel, und `Red Hat Enterprise Linux (<Kernelversion>)`, für den Einzelprozessor, angezeigt.

Treten beim SMP-Kernel Probleme auf, wählen Sie einen nicht-SMP-Kernel beim Neustart aus.

Nachdem der Bootloader der 2. Phase den zu bootenden Kernel ermittelt hat, sucht er die entsprechende Binärdatei des Kernel im `/boot`-Verzeichnis. Die eigentliche Binärdatei ist die Datei `/boot/vmlinuz-2.4.x-xx`, die den Einstellungen des Bootloaders entspricht.

Informationen zum Benutzen des Bootloaders, um dem Kernel Befehlszeilenargumente zu übergeben, finden Sie unter Kapitel 2. Informationen zum Ändern des Runlevels am GRUB- oder LILO-Prompt finden Sie unter Abschnitt 2.10.

Anschließend legt der Bootloader das entsprechende Image der *initialen RAM-Disk*, *initrd* im Speicher ab. `initrd` wird vom Kernel zum Laden der nicht kompilierten Treiber verwendet, die zum Starten des Systems erforderlich sind. Dies ist besonders wichtig, wenn Sie SCSI-Festplatten haben oder das ext3 Dateisystem [2] verwenden.

Warnung

Entfernen Sie auf gar keinen Fall das `/initrd/`-Verzeichnis aus dem Dateisystem. Wenn dieses Verzeichnis entfernt wird, kann das System nicht starten und der Kernel meldet einen gravierenden Fehler.

Sobald der Kernel und das *initrd*-Image in den Speicher geladen sind, übergibt der Bootloader die Steuerung des Bootprozesses an den Kernel.

Für einen detaillierteren Überblick des GRUB und des LILO Bootloaders, sehen Sie Kapitel 2.

1.2.2.1. Bootloader für andere Architekturen

Ist der Kernel erst einmal geladen und übergibt den Bootprozess zum `init` Befehl, erfolgt die selbe Abfolge von Events auf jeder Architektur. Der Hauptunterschied zwischen den Bootprozessen der verschiedenen Architekturen liegt deshalb in der Applikation, welche zum Finden und Laden des Kernel verwendet wird.

Die Alpha-Architektur, zum Beispiel, verwendet den aboot Bootloader, die Itanium-Architektur den ELILO Bootloader, IBM pSeries verwendet YABOOT und IBM s390 Systeme den z/IPL Bootloader.

Lesen Sie das für die jeweilige Plattform spezifische *Red Hat Enterprise Linux Installationshandbuch* für Informationen zum Konfigurieren der Bootloader.

2. Detaillierte Informationen zum Erstellen von *initrd*, sehen Sie das Kapitel *Das ext3 Dateisystem* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

1.2.3. Der Kernel

Wenn der Kernel lädt, initialisiert und konfiguriert er sofort den Arbeitsspeicher des Computers. Anschließend wird die an das System angeschlossene Hardware konfiguriert, einschließlich aller Prozessoren und E/A-Subsysteme sowie alle Speichergeräte. Dann sucht er nach dem komprimierten `initrd`-Image an einem bestimmten Speicherort im Speicher, dekomprimiert es, mountet es und lädt alle notwendigen Treiber. Danach initialisiert er die mit dem Dateisystem verbundenen virtuellen Geräte wie LVM oder Software-RAID, bevor das `initrd`-Disk-Image dekomprimiert und der gesamte Speicher freigesetzt wird, der belegt war.

Nach dem Initialisieren aller Geräte des Systems erstellt der Kernel ein root-Gerät, mountet die root-Partition als schreibgeschützt und setzt nicht verwendeten Speicher frei.

Zu diesem Zeitpunkt ist der Kernel in den Speicher geladen und betriebsbereit. Allerdings ist das System ohne die Möglichkeit für den Benutzer, sinnvolle Eingaben vorzunehmen, nicht von großem Nutzen.

Der Kernel startet den Befehl `/sbin/init`, um die Benutzerumgebung einzurichten.

1.2.4. Das Programm `/sbin/init`

Das Programm `/sbin/init` (auch `init` genannt) koordiniert den verbleibenden Bootprozess und konfiguriert die Benutzerumgebung.

Wenn `init` gestartet wird, wird es automatisch der Elternprozess aller zukünftigen, auf dem System automatisch gestarteten, Prozesse. Zuerst führt es das `/etc/rc.d/rc.sysinit`-Skript aus, das den Umgebungspfad einstellt, Swapping startet, die Dateisysteme überprüft und andere Schritte der Systeminitialisierung übernimmt. `rc.sysinit` kümmert sich im Grunde um alle Prozesse, die beim Starten des Systems durchgeführt werden müssen. Die meisten Systeme verwenden zum Beispiel eine Uhr. In diesem Fall liest `rc.sysinit` die Konfigurationsdatei `/etc/sysconfig/clock`, um die Hardware-Uhr zu initialisieren. Falls Sie über spezielle serielle Portprozesse verfügen, die ebenfalls initialisiert werden müssen, führt `rc.sysinit` die Datei `/etc/rc.serial` aus.

Anschließend führt `init` das `/etc/inittab`-Skript aus, das beschreibt, wie das System auf jedem *SysV init-Runlevel* eingerichtet werden sollte [3]. Die Datei `/etc/inittab` legt u.a. den Standard-Runlevel fest und bestimmt, dass `/sbin/update` bei jedem Start eines bestimmten Runlevels ausgeführt werden muss. [4].

Danach legt `init` die Quellfunktionsbibliothek `/etc/rc.d/init.d/functions` für das System fest. In der Datei wird festgelegt, wie Programme zu starten oder zu beenden sind und wie die PID eines Programms bestimmt werden kann.

Danach startet `init` alle Hintergrundprozesse, indem es im entsprechenden `rc`-Verzeichnis nach den Runleveln sucht, die in `/etc/inittab` als Standard festgelegt sind. Die `rc`-Verzeichnisse sind gemäß den Runleveln nummeriert, die sie darstellen. So ist zum Beispiel `/etc/rc.d/rc5.d/` das Verzeichnis für Runlevel 5.

Das Programm `init` sucht beim Starten auf Runlevel 5 im Verzeichnis `/etc/rc.d/rc5.d/`, um die Prozesse zu ermitteln, die gestartet und beendet werden müssen.

Folgend ist ein Beispiel-Listing für das Verzeichnis `/etc/rc.d/rc5.d/`:

```
K05innd -> ../init.d/innd
K05saslauthd -> ../init.d/saslauthd
K10psacct -> ../init.d/psacct
K10radiusd -> ../init.d/radiusd
K12mysqld -> ../init.d/mysqld
K15httpd -> ../init.d/httpd
```

3. Weitere Informationen zu SysV init Runleves finden Sie unter Abschnitt 1.4.
4. Das `update`-Programm gibt fehlerhafte Buffer auf der Festplatte wieder frei.

```
K15postgresql -> ../init.d/postgresql
K16rarpd -> ../init.d/rarpd
K20iscsi -> ../init.d/iscsi
K20netdump-server -> ../init.d/netdump-server
K20nfs -> ../init.d/nfs
K20tomcat -> ../init.d/tomcat
K24irda -> ../init.d/irda
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
K34dhcrelay -> ../init.d/dhcrelay
K34yppasswdd -> ../init.d/yppasswdd
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
K35winbind -> ../init.d/winbind
K36lisa -> ../init.d/lisa
K45arpwatch -> ../init.d/arpwatch
K45named -> ../init.d/named
K45smartd -> ../init.d/smartd
K46radvd -> ../init.d/radvd
K50netdump -> ../init.d/netdump
K50snmpd -> ../init.d/snmpd
K50snmptrapd -> ../init.d/snmptrapd
K50tux -> ../init.d/tux
K50vsftpd -> ../init.d/vsftpd
K54pxe -> ../init.d/pxe
K61ldap -> ../init.d/ldap
K65kadmin -> ../init.d/kadmin
K65kprop -> ../init.d/kprop
K65krb524 -> ../init.d/krb524
K65krb5kdc -> ../init.d/krb5kdc
K70aep1000 -> ../init.d/aep1000
K70bcm5820 -> ../init.d/bcm5820
K74ntpd -> ../init.d/ntpd
K74ypserv -> ../init.d/ypserv
K74ypxfrd -> ../init.d/ypxfrd
K84bgpd -> ../init.d/bgpd
K84ospf6d -> ../init.d/ospf6d
K84ospfd -> ../init.d/ospfd
K84ripd -> ../init.d/ripd
K84ripngd -> ../init.d/ripngd
K85zebra -> ../init.d/zebra
K92ipvsadm -> ../init.d/ipvsadm
K95firstboot -> ../init.d/firstboot
S00microcode_ctl -> ../init.d/microcode_ctl
S08ip6tables -> ../init.d/ip6tables
S08iptables -> ../init.d/iptables
S09isdn -> ../init.d/isdn
S10network -> ../init.d/network
S12syslog -> ../init.d/syslog
S13irqbalance -> ../init.d/irqbalance
S13portmap -> ../init.d/portmap
S14nfslock -> ../init.d/nfslock
S17keytable -> ../init.d/keytable
S20random -> ../init.d/random
S24pcmcia -> ../init.d/pcmcia
S25netfs -> ../init.d/netfs
S26apmd -> ../init.d/apmd
```

```
S28autofs -> ../init.d/autofs
S44acpid -> ../init.d/acpid
S55sshd -> ../init.d/sshd
S56rawdevices -> ../init.d/rawdevices
S56xinetd -> ../init.d/xinetd
S59hpoj -> ../init.d/hpoj
S80sendmail -> ../init.d/sendmail
S85gpm -> ../init.d/gpm
S90canna -> ../init.d/canna
S90crond -> ../init.d/crond
S90cups -> ../init.d/cups
S90FreeWnn -> ../init.d/FreeWnn
S90xfs -> ../init.d/xfs
S95atd -> ../init.d/atd
S97rhnsd -> ../init.d/rhnsd
S99local -> ../rc.local
S99mdmonitor -> ../init.d/mdmonitor
```

Wie Sie sehen, befindet sich keines der Skripte, die die Dienste starten und beenden, im Verzeichnis `/etc/rc.d/rc5.d/`. Vielmehr sind alle Dateien in `/etc/rc.d/rc5.d/` *symbolische Links*, die auf Skripte im `/etc/rc.d/init.d/`-Verzeichnis zeigen. Symbolische Links werden in allen `rc`-Verzeichnissen verwendet, so dass die Runlevel durch Erstellen, Ändern und Löschen der symbolischen Links neu konfiguriert werden können, ohne dass die aktuellen Skripte davon betroffen werden, auf die sie verweisen.

Der Name jedes symbolischen Links beginnt entweder mit einem `K` oder einem `S`. Die `K`-Links sind Prozesse, die auf diesem Runlevel entfernt werden, während die Links gestartet werden, die mit einem `S` beginnen.

Zuerst beendet der Befehl `init` alle symbolischen `K`-Links im Verzeichnis mit Hilfe des Befehls `/etc/rc.d/init.d/<`*`Befehl`*`> stop`, wobei `<`*`Befehl`*`>` der zu beendende Prozess ist. Anschließend werden alle symbolischen `S`-Links mit Hilfe von `/etc/rc.d/init.d/<`*`Befehl`*`> start` gestartet.

Tipp

Wenn das System den Bootvorgang beendet hat, können Sie sich als root anmelden und dieselben Skripte zum Starten und Beenden der Dienste ausführen. So beendet zum Beispiel der Befehl `/etc/rc.d/init.d/httpd stop` den Apache HTTP Server.

Alle symbolischen Links sind nummeriert, um die Startreihenfolge festzulegen. Sie können die Reihenfolge ändern, in der die Dienste gestartet oder beendet werden, indem Sie die Nummerierung ändern. Je kleiner die Nummer, desto früher wird gestartet. Die symbolischen Links mit derselben Nummer werden in alphabetischer Reihenfolge gestartet.

Anmerkung

Als eine der letzten Aktionen führt das Programm `init` alle Skripte aus, die sich in `/etc/rc.d/rc.local` befinden. Diese Datei ist nützlich für das Anpassen des Systems. Für mehr zur Verwendung von `rc.local` lesen Sie Abschnitt 1.3.

Nachdem der Befehl `init` das entsprechende `rc`-Verzeichnis für das Runlevel verarbeitet hat, sucht das Skript `/etc/inittab` einen `/sbin/mingetty`-Prozess für jede virtuelle Konsole (Anmelde-

bildschirme), die dem Runlevel zugewiesen ist. Runlevel 2 bis 5 rufen alle sechs virtuellen Konsolen auf, während Runlevel 1 (Einzelbenutzermodus) nur eine aufruft und Runlevel 0 und 6 gar keine. Der `/sbin/mingetty`-Prozess öffnet Kommunikationswege zu *tty*-Geräten[5],legt die Modi fest, druckt den Anmeldebildschirm, ruft den Benutzernamen ab und initiiert den Anmeldeprozess für den Benutzer.

Auf Runlevel 5 führt `/etc/inittab` das Skript `/etc/X11/prefdm` aus. Das `prefdm`-Skript führt den gewünschten X-Desktop-Manager[6] aus — `gdm`, `kdm` oder `xdm`, je nach Inhalt der Datei `/etc/sysconfig/desktop`.

Zu diesem Zeitpunkt ist das System im Runlevel 5 und zeigt den Anmeldebildschirm an.

1.3. Ausführen von zusätzlichen Programmen zum Zeitpunkt des Bootens

Das Skript `/etc/rc.d/rc.local` wird vom Befehl `init` zum Zeitpunkt des Bootens ausgeführt, nachdem die restliche Initialisierung abgeschlossen ist, sowie bei Änderungen der Runlevel. Das Hinzufügen von Befehlen zu diesem Skript ist ein einfacher Weg, notwendige Tasks auszuführen, wie das Starten von speziellen Services oder das Initialisieren von Geräten, ohne ein Schreiben komplizierter Installationsskripte im Verzeichnis `/etc/rc.d/init.d/` und das Erzeugen symbolischer Links zu erfordern.

Wenn Sie das Einstellen von seriellen Ports benötigen, können Sie außerdem `/etc/rc.serial` erstellen und ändern, so dass es zum Zeitpunkt des Bootens automatisch ausgeführt wird. Dieses Skript kann eine Vielzahl von `setserial`-Befehlen ausführen, um die seriellen Ports des Systems speziell zu konfigurieren. Auf der `setserial`-man-Seite finden Sie weitere Informationen hierzu.

1.4. SysV Init Runlevels

Das SysV init Runlevel System stellt einen Standardprozess zur Kontrolle, welche Programme von `init` während des Initialisierens des Runlevels gestartet oder angehalten werden, bereit. SysV wurde gewählt, da es einfacher zu benutzen und flexibler ist als der herkömmliche BSD-Style-Init-Prozess.

Die Konfigurationsdateien für SysV init befinden sich im Verzeichnis `/etc/rc.d/`. In diesem Verzeichnis befinden sich die Skripte `rc`, `rc.local`, `rc.sysinit` und, optional, `rc.serial` sowie die folgenden Verzeichnisse:

```
init.d/
rc0.d/
rc1.d/
rc2.d/
rc3.d/
rc4.d/
rc5.d/
rc6.d/
```

Das Verzeichnis `init.d/` enthält die vom Befehl `/sbin/init` zum Steuern der Dienste verwendeten Skripte. Jedes der nummerierten Verzeichnisse stellt die sechs Runlevel dar, die standardmäßig unter Red Hat Enterprise Linux konfiguriert sind.

5. Weitere Informationen zu `tty`-Geräten finden Sie unter Abschnitt 5.3.11.
6. Sehen Sie Abschnitt 7.5.2 für weitere Informationen zu Display-Managern.

1.4.1. Runlevels

Runlevels sind ein Zustand, oder *Modus*, durch die im SysV Verzeichnis `/etc/rc.d/rc<x>.d/` enthaltenen Services definiert werden, wobei `<x>` die Nummer des Runlevels ist.

Die Idee hinter SysV init Runlevels basiert auf der Gegebenheit, dass verschiedene Systeme auf verschiedene Weise verwendet werden können. Ein Server, zum Beispiel, ist effizienter, wenn kein X Window System läuft und Systemressourcen verschwendet. Zu anderen Zeiten muss z.B. ein Systemadministrator das System auf einem niedrigeren Runlevel betreiben, um diagnostische Aufgaben zu erledigen, wie das Beheben von korrumpierten Dateisystemen in Runlevel 1, wenn keine anderen Benutzer auf dem System sein können.

Die Eigenschaften eines gegebenen Runlevel bestimmen, welche Services von `init` angehalten und gestartet werden. Runlevel 1 (Einzelbenutzer-Modus), zum Beispiel, hält alle Netzwerk-Services, während Runlevel 3 diese startet. Durch die Angabe, bei welchem Runlevel spezifische Services angehalten oder gestartet werden, kann `init` schnell den Modus der Maschine ändern, ohne dass der Benuzter diese Services manuell starten oder anhalten müsste.

Die folgenden Runlevels sind in Red Hat Enterprise Linux standardmäßig definiert:

- `0` — Anhalten
- `1` — Einzelbenutzer Textmodus
- `2` — Nicht belegt (benutzerspezifisch)
- `3` — Vollständiger Mehrbenutzer Textmodus
- `4` — Nicht belegt (benutzerspezifisch)
- `5` — Vollständiger Mehrbenutzer graphischer Modus (mit einem X-basierten Anmeldebildschirm)
- `6` — Neu booten

Im allgemeinen arbeitet Red Hat Enterprise Linux auf Runlevel 3 oder Runlevel 5 — und zwar jeweils im vollständigen Mehrbenutzermodus. Die Runlevels 2 und 4 können vom Benutzer definiert werden, da diese ja nicht verwendet werden.

Der Standard-Runlevel wird in `/etc/inittab` bestimmt. Um für Ihr System den Standard-Runlevel herauszufinden, müssen Sie eine Zeile suchen, die der unten angegebenen `/etc/inittab` ähnelt:

```
id:5:initdefault:
```

Der standardmäßige Runlevel im obigen Beispiel ist fünf, wie die Nummer hinter dem Doppelpunkt angibt. Um diesen zu ändern, bearbeiten Sie `/etc/inittab` als root.

Warnung

Seien Sie beim Bearbeiten von `/etc/inittab` vorsichtig. Einfache Schreibfehler können dazu führen, dass das System nicht mehr booten kann. Sollte dies vorkommen, verwenden Sie entweder eine Bootdiskette, treten Sie in den Einzelbenutzermodus ein, oder geben Sie Rescue-Modus ein, um Ihren Computer zu booten und die Datei zu reparieren.

Für mehr Information zu Einzelbenutzer und Rescue-Modus, sehen Sie Kapitel *Basic System Recovery* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Es ist möglich, den Default-Runlevel zur Bootzeit zu ändern, indem Sie die Argumente ändern, die der Bootloader dem Kernel übergibt. Weitere Informationen zum Ändern der Runlevel zur Bootzeit finden Sie unter Abschnitt 2.10.

1.4.2. Runlevel Utilities

Einer der besten Wege, die Runlevels zu konfigurieren, ist die Verwendung eines *Initscript Utility*. Diese Tools erleichtern den Task, die Dateien in der SysV init Verzeichnishierarchie zu warten und nimmt es den Systemadministratoren ab, die große Anzahl von symbolischen Links in den Unterverzeichnissen von `/etc/rc.d/` direkt ändern zu müssen.

Red Hat Enterprise Linux stellt drei dieser Utilities zur Verfügung:

- `/sbin/chkconfig` — Das `/sbin/chkconfig` Utility stellt ein einfaches Befehlszeilentool für die Pflege der `/etc/rc.d/init.d/`-Verzeichnishierarchie zur Verfügung.
- **/sbin/ntsysv** — Das ncurses-basierte **/sbin/ntsysv** Utility stellt eine interaktive textbasierte Oberfläche zur Verfügung, was einige benutzerfreundlicher finden, als die Befehlszeilenoberfläche von `chkconfig`.
- **Services Configuration Tool** — Das graphische **Services Configuration Tool** (`redhat-config-services`) Programm ist ein flexibles GTK2-basiertes Utility zum Konfigurieren der Runlevels.

Im Kapitel *Controlling Access to Services* im *Red Hat Enterprise Linux Handbuch zur System-Administration* finden Sie weitere Informationen zu diesen Tools.

1.5. Herunterfahren

Um Red Hat Enterprise Linux herunterzufahren, kann der root-Benutzer den Befehl `/sbin/shutdown` ausführen. Die man-Seiten zu `shutdown` enthalten eine vollständige Liste von Optionen. Hier sind die zwei am häufigsten verwendeten:

```
/sbin/shutdown -h now
/sbin/shutdown -r now
```

Nachdem das System vollständig heruntergefahren wurde, hält die Option `-h` den Rechner an, und die Option `-r` startet diesen neu.

Benutzer von PAM-Konsolen können die Befehle `reboot` und `halt` verwenden, um das System herunterzufahren, solange das System in den Runlevels 1 bis 5 ist. Für weitere Informationen zur Verwendung von PAM-Konsolen, sehen Sie Abschnitt 13.7.

Sollte der Computer sich nicht selbst herunterfahren, seien Sie vorsichtig und schalten Sie den Computer nicht aus, bis eine Nachricht erscheint, dass das System angehalten wurde.

Wenn Sie dies nicht tun und den Computer ausschalten, bevor diese Meldung erscheint, kann auf einigen Partitionen noch ein Mount bestehen, was zur Korruption von Daten führen kann.

redhat.

Kapitel 2.

Bootloader

Wenn ein Computer mit Red Hat Enterprise Linux angeschaltet wird, muss das Operationssystem über ein spezielles Programm namens *Bootloader* geladen werden. Ein Bootloader ist in der Regel auf der ersten Festplatte des Systems oder auf einem anderen Mediengerät installiert und ist nur für das Laden des Linux-Kernels und seiner erforderlichen Dateien oder in manchen Fällen für das Laden anderer Betriebssysteme in den Speicher verantwortlich.

2.1. Bootloader und Systemarchitektur

Jede Rechnerarchitektur, die Red Hat Enterprise Linux ausführen kann, verwendet einen anderen Bootloader. Die folgende Tabelle listet die Bootloader auf, die für jede Architektur verhanden sind.

Systemarchitektur	Bootloader
AMD® AMD64	GRUB
IBM® eServer™ iSeries™	OS/400®
IBM® eServer™ pSeries™	YABOOT
IBM® S/390®	z/IPL
IBM® eServer™ zSeries®	z/IPL
Intel® Itanium™	ELILO
x86	GRUB oder LILO

Tabelle 2-1. Bootloader für Systemarchitekturen

In diesem Kapitel werden Befehle und Konfigurationsoptionen der beiden Bootloader besprochen, die mit Red Hat Enterprise Linux für die x86-Architektur geliefert werden: GRUB und LILO.

2.2. GRUB

GNU GRand Unified Bootloader oder GRUB ist ein Programm, mit dem der Benutzer das Betriebssystem oder den Kernel auswählen kann, das bzw. der beim Systemstart geladen werden soll. Desweiteren kann der Benutzer Argumente an den Kernel übergeben.

2.2.1. GRUB und der x86-Bootprozess

In diesem Abschnitt wird die spezifische Rolle von GRUB beim Booten eines x86-Systems ausführlich beschrieben. Detaillierte Informationen zum gesamten Bootprozess finden Sie unter Abschnitt 1.2.

GRUB lädt sich selbst in folgenden Phasen in den Speicher:

1. *Der Stage 1 oder primäre Bootloader wird aus dem MBR vom BIOS in den Speicher gelesen*[1]. Der primäre Bootloader nimmt weniger als 512 Bytes Plattenplatz im MBR in Anspruch. Seine einzige Aufgabe ist das Laden des Stage 1.5 oder Stage 2 Bootloaders.

1. Weitere Informationen zum BIOS und MBR finden Sie unter Abschnitt 1.2.1.

2. *Der Stage 1.5 Bootloader wird vom Stage 1-Bootloader in den Speicher eingelesen, wenn dies notwendig ist.* Für manche Hardware ist ein Zwischenschritt beim Aufrufen des Stage 2 Bootloaders erforderlich. Dies trifft manchmal zu, wenn die `/boot`-Partition 1024 Zylinder auf der Festplatte überschreitet oder wenn LBA-Modus verwendet wird. Der Stage 1.5 Bootloader befindet sich entweder auf der `/boot/`- Partition oder auf einem kleinen Teil des MBR und der `/boot` Partition.
3. *Der Stage 2 oder sekundäre Bootloader wird in den Speicher gelesen.* Der sekundäre Bootloader zeigt die Menü- und Befehlsumgebung von GRUB an. Mit dieser Oberfläche können Sie das zu startende Betriebssystem bzw. den Linux-Kernel auswählen, Argumente an den Kernel weiterleiten oder sich die Systemparameter anzeigen lassen.
4. *Der sekundäre Bootloader liest das Betriebssystem bzw. den Kernel und* `initrd` *in den Speicher.* Sobald GRUB festlegt, welches Betriebssystem gestartet werden soll, lädt er es in den Speicher und übergibt die Steuerung der Rechners an das Betriebssystem.

Diese zum Starten von Red Hat Enterprise Linux verwendete Bootmethode wird *direktes Laden* genannt, da der Bootloader das Betriebssystem direkt lädt. Zwischen dem Bootloader und dem Kernel ist keine Zwischenstufe vorhanden.

Der von den anderen Betriebssystemen verwendete Bootprozess kann von dem hier beschriebenen abweichen. For example werden die the Microsoft® Windows ® Operationssysteme und andere Systeme mit *chain loading* geladen. Bei dieser Methode verweist der MBR einfach auf den ersten Sektor der Partition, auf der das Betriebssystem installiert ist. Dort befinden sich die für das Starten des Betriebssystems erforderlichen Dateien.

GRUB unterstützt sowohl die direkte als auch die verkettete Lademethode, wodurch fast alle Betriebssysteme gestartet werden können.

Warnung

Während der Installation überschreiben DOS und Windows von Microsoft den MBR komplett und löschen somit alle vorhandenen Bootloader. Wird ein duales Bootsystem erstellt, wird empfohlen, das Betriebssystem von Microsoft zuerst zu installieren.

2.2.2. Funktionen von GRUB

GRUB enthält zahlreiche Funktionen, die im Vergleich zu anderen für die x86-Architektur verfügbaren Bootloadern vorteilhaft sind. Nachfolgend ist eine Liste mit den wichtigsten Funktionen angeführt:

- *GRUB liefert auf x86-Rechnern eine echte, auf Befehlen basierende vor-OS-Umgebung.* Dies verleiht dem Benutzer maximale Flexibilität beim Laden der Betriebssysteme mit bestimmten Optionen bzw. beim Sammeln von Informationen über das System. Viele nicht-x86-Architekturen verwenden seit Jahren vor-OS-Umgebungen, die das Starten des Systems von einer Befehlszeile aus ermöglichen. Einige Befehlsfunktionen stehen mit LILO oder anderen x86-Bootloadern zur Verfügung, GRUB bietet jedoch eine größere Anzahl solcher Funktionen.
- *GRUB unterstützt den Logical Block Addressing (LBA) Modus.* LBA übergibt die Adressen-Konvertierung, die dazu dient, Dateien zu suchen, in der Firmware der Festplatte, und wird auf vielen IDE- und allen SCSI-Festplatten verwendet. In Zeiten vor LBA stießen Bootloader auf die 1024-Zylindergrenze des BIOS, über der das BIOS keine Dateien finden konnte. Die LBA-Unterstützung ermöglicht GRUB, Betriebssysteme von Partitionen oberhalb der 1024-Zylindergrenze zu booten, sofern das System-BIOS den LBA-Modus unterstützt. Die meisten modernen BIOS-Versionen unterstützen den LBA-Modus.

- *GRUB kann ext2-Partitionen lesen.* Deswegen kann GRUB bei jedem Systemstart auf seine Konfigurationsdatei `/boot/grub/grub.conf` zugreifen und damit umgehen, eine neue Version des Stage 1 Bootloaders auf den MBR schreiben zu müssen, wenn die Konfiguration geändert wird. GRUB muss nur dann neu auf dem MBR installiert werden, wenn die physische Speicherstelle der `/boot`- Partition auf der Platte verschoben wird. Detaillierte Informationen zum Installieren von GRUB auf den MBR finden Sie unter Abschnitt 2.3.

2.3. Installation von GRUB

Wenn Sie GRUB während des Installationsprozesses nicht installiert haben, können Sie ihn später installieren. Er wird nach dem Installieren automatisch zum standardmäßigen Bootloader.

Vor der Installation von GRUB sollten Sie sicherstellen, dass Sie das neueste GRUB-Paket haben. Sie können auch das GRUB-Paket von den Installations-CD-ROMs verwenden. Informationen zum Installieren von Paketen finden Sie im Kapitel *Paket-Management mit RPM* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Öffnen Sie nach der Installation des GRUB-Pakets einen Root-Shell-Prompt und führen Sie den Befehl `/sbin/grub-install <Speicherort>` aus, wobei `<Speicherort>` der Speicherort ist, in den der Stage 1 GRUB-Bootloader installiert werden soll. Z.B installiert der folgende Befehl Grub in den MDR des Master-IDE-Gerätes auf der primären IDE-Sammelleitung.

```
/sbin/grub-install /dev/hda
```

Beim nächsten Systemstart wird das grafische Bootloader-Menü von GRUB angezeigt, bevor der Kernel in den Speicher geladen wird.

Wichtig

Wenn GRUB auf einem RAID 1 Array installiert wird, kann passieren, dass sich das System im Falle eines Plattenversagens nicht mehr starten lässt. Eine nicht unterstützte Hilfestellung wir online unter der folgenden URL geboten:

http://www.dur.ac.uk/a.d.stribblehill/mirrored_grub.html

2.4. GRUB-Terminologie

Zu den grundlegenden Kenntnissen vor der Verwendung von GRUB gehört, wie das Programm Geräte wie Festplatten und Partitionen anspricht. Diese Informationen sind insbesondere dann wichtig, wenn GRUB zum Starten mehrerer Betriebssysteme konfiguriert werden soll.

2.4.1. Gerätenamen

Wenn Sie sich auf ein bestimmtes Gerät mit GRUB beziehen, verwenden Sie folgendes Format (beachten Sie, dass die Klammern und Kommas syntaktisch sehr wichtig sind):

```
(<type-of-device><bios-device-number>,<partition-number>)
```

`<Gerätetyp>` legt den Typ des Gerätes fest, von dem aus GRUB startet. Die zwei gebräuchlichsten Optionen sind `hd` für eine Festplatte oder `fd` für eine 3.5 Diskette. Es gibt auch einen weniger verwendeten Geräte-Typ für eine Netzwerkplatte, `nd` genannt. Anweisungen für das Konfigurieren von GRUB zum Hochfahren über ein Netzwerk finden Sie unter http://www.gnu.org/manual/grub/.

Die <*Bios-Gerätenummer*> ist die Nummer für die BIOS-Einrichtung. Die primäre IDE-Festplatte trägt die Nummer0 und eine sekundäre Festplatte trägt die Nummer1. Diese Syntax ist im Groben jener ähnlich, die der Kernel für Geräte verwendet. Z.B. ist a in hda für den Kernel analog zu 0 in hd0 für GRUB, b in hdb ist analog zu 1 in hd1 und so weiter.

Die <*Partitionsnummer*>bezieht sich auf die Nummer einer spezifischen Partition auf einem Plattengerät. Wie die <*BIOS-Gerätenummer*> beginnt die Nummerierung bei den meisten Partitionstypen bei 0. BSD-Partitionen werden allerdings mit Buchstaben festgelegt, wobei a mit 0 korrespondiert, b mit 1 und so weiter.

Tipp

Das Nummerierungsystem für Geräte beginnt bei GRUB immer mit 0,nicht mit1. Fehler bei dieser Unterscheidung gehören zu den häufigsten Fehlern, die von neuen GRUB- Benutzern begangen werden.

Ein Beispiel: wenn ein System mehr als eine Festplatte hat, bezeichnet GRUB die erste Festplatte als (hd0) und die zweite als (hd1). Ebenso bezeichnet GRUB die erste Partition auf der ersten Platte als (hd0,0) und die dritte Partition auf der zweiten Platte als (hd1,2).

Bei GRUB gelten generell die folgenden Regeln für die Bezeichnung von Geräten und Partitionen:

- Unabhängig davon, ob es sich bei den Festplatten um IDE- oder SCSI-Festplatten handelt, beginnen alle Festplatten mit den Buchstaben hd. Die Buchstaben fd hingegen werden zur Bezeichnung von Disketten verwendet.
- Um ein ganzes Gerät ohne Berücksichtigung seiner Partitionen anzugeben, lassen Sie einfach das Komma und die Partitionsnummer weg. Dies ist dann wichtig, wenn Sie GRUB anweisen, den MBR für eine bestimmte Festplatte zu konfigurieren. Beispielsweise gibt (hd0) den MBR auf dem ersten Gerät an, und (hd3) gibt den MBR auf dem vierten Gerät an.
- Wenn ein System über mehrere Festplatten verfügt, muss deren Startreihenfolge gemäß BIOS bekannt sein. Dies ist einfach, wenn das System nur IDE- oder SCSI-Festplatten besitzt. Wenn jedoch eine Mischung aus verschiedenen Geräten vorliegt, ist es wichtig, dass zuerst auf jenes Gerät zugegriffen wird, auf dem sich die Boot-Partition befindet.

2.4.2. Dateinamen und Blocklisten

Wenn Sie Befehle in GRUB eingeben, die sich auf eine Datei beziehen, wie z.B. eine Menüliste, ist es notwendig, gleich nach der Geräte- und Partitionsnummer einen absoluten Dateipfad festzulegen.

Im Folgenden wird die Struktur eines solchen Befehls gezeigt:

(<*device-type*><*device-number*>,<*partition-number*>)<*/path/to/file*>

Ersetzen Sie bei diesem Beispiel <*Gerätetyp*> mit hd, fd, oder nd. Ersetzen Sie <*Gerätenummer*> mit der Ganzzahl für das Gerät. Ersetzen Sie <*/Pfad/zur/Datei*> mit einem absoluten Pfad in Bezug zur höchsten Ebene des Gerätes.

In GRUB können auch Dateien festgelegt werden, die eigentlich nicht im Dateisystem angezeigt werden. Ein Beispiel ist ein Kettenloader, der sich in den ersten paar Blöcken einer Partition befindet. Zum Laden solcher Dateien muss eine *Blockliste* zur Verfügung gestellt werden, die Block für Block angibt, an welcher Stelle der Partition sich die Datei befindet. Da eine Datei oft aus mehreren Blocksätzen besteht, werden die Blocklisten auf eine ganz bestimmte Art und Weise geschrieben. Jeder Block, der die Datei enthält, wird durch eine Offset-Anzahl von Blöcken festgelegt, gefolgt von der Anzahl

der Blöcke ab diesem Offset-Punkt. Die Block-Offsets werden in Reihenfolge und durch Kommas getrennt aufgelistet.

Folgend ist ein Beispiel einer Blockliste:

```
0+50,100+25,200+1
```

Diese Probe-Blockliste legt eine Datei fest, die beim ersten Block der Partition beginnt und die Blöcke 0 bis 49, 99 bis 124 und 199 verwendet.

Blocklisten schreiben zu können ist dann sehr nützlich, wenn GRUB zum Laden von Betriebssystemen verwendet wird, die das verkettete Laden benutzen. Sie können den Offset an Blöcken weglassen, wenn Sie bei Block 0 starten. Beispiel: die Kettenlade-Datei auf der ersten Partition der ersten Festplatte würde somit folgenden Namen besitzen:

```
(hd0,0)+1
```

Im Folgenden wird der Befehl `chainloader` mit einer ähnlichen Blocklisten-Bezeichnung in der GRUB-Befehlszeile gezeigt, nachdem Sie als root das korrekte Gerät und Partition eingestellt haben:

```
chainloader +1
```

2.4.3. Das Root-Dateisystem und GRUB

Der Begriff *Root-Dateisystem* hat bei GRUB eine andere Bedeutung. Es ist wichtig zu beachten, dass das Root-Dateisystem von GRUB nichts mit dem Root-Dateisystem von Linux zu tun hat.

Das GRUB Root-Dateisystem ist die höchste Ebene des bestimmten Gerätes. Z.B. die Image-Datei `(hd0,0)/grub/splash.xpm.gz` befindet sich im `/grub/` Verzeichnis auf der höchsten Ebene (oder Root) der `(hd0,0)` Partition (die eigentlich die `/boot/` Partition für das System ist).

Nachdem GRUB die root-Partition geladen hat, die der `/boot`-Partition entspricht und den Linux-Kernel enthält, kann der Befehl `kernel` mit dem Speicherort der Kerneldatei als Option ausgeführt werden. Sobald der Linux-Kernel bootet, richtet er ein eigenes root-System ein, das Linux-Benutzern bekannt ist. Das ursprüngliche root-Dateisystem von GRUB und die Mounts sind bereits vergessen. Sie dienten lediglich dem Booten der Kerneldatei.

Weitere Informationen zu den Befehlen `root` und `kernel` finden Sie unter Abschnitt 2.6.

2.5. GRUB-Oberflächen

GRUB bietet drei Oberflächen, die unterschiedliche Stufen an Funktionalität bieten. Jede einzelne Oberfläche ermöglicht das Booten des Linux Kernels oder eines anderen Betriebssystems.

Dabei handelt es sich um folgende Schnittstellen:

Menüoberfläche

Wurde GRUB vom Installationsprogramm konfiguriert, wird automatischdiese Oberfläche als Standard angezeigt. Es wird ein Menü mit vorkonfigurierten Betriebssystemen oder Kerneln als Liste nach Namen geordnet angezeigt. Anhand der Pfeiltasten können Sie eine andere Option als die Standardauswahl wählen. Drücken Sie die [Enter] Taste, um diese Option zu booten. Es kann auch eine Zeit eingestellt sein, nach der GRUB mit dem Laden der Standardoption beginnt.

Drücken Sie in der Menüoberfläche die Taste [e], um die Oberfläche des Eintrag-Editors aufzurufen, bzw. die Taste [c], um eine Befehlszeilenoberfläche zu laden.

Weitere Informationen zum Konfigurieren dieser Oberfläche finden Sie unter Abschnitt 2.7.

Oberfläche Menüeintrag-Editor

Um auf den Menüeintrag-Editor zuzugreifen, drücken Sie die Taste [e] im Bootloader-Menü. Die GRUB-Befehle für diesen Eintrag werden hier angezeigt, und die Benutzer haben die Möglichkeit, diese Befehlszeilen vor dem Starten des Betriebssystems durch Hinzufügen einer Befehlszeile ([o] fügt die neue Zeile nach der aktuellen Zeile ein, [O] davor), durch Bearbeiten ([e]) oder Löschen ([d]) zu ändern.

Nachdem die gewünschten Änderungen an den Zeilen vorgenommen wurden, können Sie die Taste [b] drücken, um die Befehle auszuführen und das Betriebssystem zu booten. Mittels der Taste [Esc] werden die Änderungen verworfen und die Standardmenüoberfläche geladen. Über die Taste [c] wird die Befehlszeilenoberfläche geladen.

Tipp

Weitere Informationen zum Ändern der Runlevel mit GRUB unter Verwendung des Menüeintrag-Editors finden Sie unter Abschnitt 2.10.

Befehlszeilenoberfläche

Die Befehlszeile ist die einfachste GRUB-Oberfläche, die gleichzeitig auch die größte Kontrolle bietet. Die Befehlszeile ermöglicht es, alle relevanten GRUB-Befehle einzugeben und diese anschließend durch Drücken der [Enter-Taste] auszuführen. Diese Oberfläche bietet einige erweiterte, shell-ähnliche Funktionen, einschließlich der auf Kontext basierenden Verwendung der Taste [Tab] zur Zeilenvervollständigung sowie den Kombinationen mit der Taste [Strg] bei der Eingabe von Befehlen (beispielsweise [Strg]-[a], wenn Sie zum Anfang einer Zeile springen möchten, und [Strg]-[e], wenn Sie zum Ende einer Zeile springen möchten). Darüber hinaus funktionieren die Tasten [Pos1], [Ende] und [Entf] wie in der `bash`-Shell.

Eine Liste mit gebräuchlichen Befehlen finden Sie unter Abschnitt 2.6.

2.5.1. Lade-Reihenfolge der Oberflächen

Wenn die GRUB-Umgebung mit dem Laden des Bootloaders der zweiten Phase beginnt, sucht diese nach der Konfigurationsdatei. Wird die Konfigurationsdatei gefunden, wird diese verwendet, um die Menüliste zu erstellen und die Bootmenüoberfläche anzuzeigen.

Kann die Konfigurationsdatei nicht gefunden oder nicht gelesen werden, lädt GRUB die Befehlszeilenoberfläche, in welcher der Benutzer Befehle eingeben kann, um den Bootprozess abzuschliessen.

Wenn die Konfigurationsdatei ungültig ist, druckt GRUB den Fehler und fordert zur Eingabe auf. Dies kann sehr nützlich sein, da die Benutzer auf diese Weise genau sehen, wo das Problem aufgetreten ist, und die Datei entsprechend korrigieren können. Durch Drücken einer beliebigen Taste wird die Menüoberfläche erneut geladen, wo die entsprechende Menüoption bearbeitet und der Fehler gemäß der Angabe von GRUB korrigiert werden kann. Schlägt die Korrektur fehl, meldet GRUB den Fehler, und die Menüoberfläche wird neu geladen.

2.6. GRUB-Befehle

GRUB bietet eine Reihe nützlicher Befehle auf seiner Befehlszeilenoberfläche. Nach dem Namen einiger dieser Befehle können Optionen eingegeben werden. Diese Optionen sind vom Befehl und anderen Optionen auf derselben Zeile durch Leerzeichen zu trennen.

In der folgenden Liste sind nützliche Befehle aufgeführt:

- `boot` — Bootet das Betriebssystem oder den Kettenloader, das/der zuletzt geladen wurde.

- `chainloader <Dateiname>` — Lädt die angegebene Datei als Kettenloader. Wenn sich die Datei im ersten Sektor der angegebenen Partition befindet, verwenden Sie stattdesses `+1` als Dateinamen.

  Im Folgenden ein Beispiel für einen `chainloader` Befehl:
  ```
  chainloader +1
  ```

- `displaymem` — Zeigt den derzeitigen Speicherbedarf entsprechend den Informationen des BIOS an. Dies ist besonders zum Ermitteln des RAM eines Systems vor dem Booten nützlich.

- `initrd </path/to/initrd>` — Ermöglicht die Angabe einer initialen RAM-Disk, die beim Booten verwendet wird. Eine `initrd` ist erforderlich, wenn der Kernel bestimmte Module zum ordnungsgemäßen Starten benötigt. Dies ist zum Beispiel dann der Fall, wenn die root-Partition mit dem Dateisystem ext3 formatiert wurde.

  Im Folgenden ein Bespiel für einen `initrd` Befehl:
  ```
  initrd /initrd-2.4.21.ent.img
  ```

- `install <stage-1> <install-disk> <stage-2> p config-file` — Installiert GRUB in den System-MBR.

  - `<stage-1>` — Spezifiziert Gerät, Partition, und Datei, wo das erste Boot-Loader Image gefunden werden kann, z.B. `(hd0,0)/grub/stage1`.
  - `<install-disk>` — Gibt die Platte an, auf welcher der Stage 1 Boot-Loader installiert sein sollte, z.B. `(hd0)`.
  - `<stage-2>` — Übergibt dem Stage 1 Boot-Loader den Ort, an welchem sich der Stage 2 Boot-Loader befindet, z.B. `(hd0,0)/grub/stage2`.
  - `p <config-file>` — Diese Option weist den `install` Befehl an, nach der Konfigurationsdatei des Menüs, das durch `<config-file>` spezifiziert ist, zu suchen. Zum Beispiel `(hd0,0)/grub/grub.conf`.

  Warnung

  Der `install` Befehl überschreibt alle Informationen, die sich bereits auf dem MBR befinden.

- `kernel </path/to/kernel> <option-1> <option-N> ...` — Gibt die Kernel-Datei an, die geladen werden soll, wenn das Betriebssystem hochgefahren wird. Ersetzen Sie `</path/to/kernel>` mit einem absoluten Pfad von der Partition, die durch den Root-Befehl festgelegt ist. Ersetzen Sie `<option-1>` mit Optionen für den Linux-Kernel, z.B. `root=/dev/hda5`, um das Gerät festzulegen, auf dem sich die Root-Partition für das System befindet. Dem Kernel können mit einer Lehrzeichen-Trennliste mehrere Optionen weitergegeben werden.

  Im Folgenden das Beispiel eines `kernel` Befehls:
  ```
  kernel /vmlinuz-2.4.21 root=/dev/hda5
  ```

  Die Option im vorhergehenden Beispiel legt fest, dass sich das Root-Dateisystem für Linux auf der `hda5` Partition befindet.

- `root (<device-type><device-number>,<partition>)` — Konfiguriert die Root-Partition für GRUB, z.B. `(hd0,0)` und mountet die Partition.

  Im Folgenden ein Beispiel für einen `root` Befehl:
  ```
  root (hd0,0)
  ```

- `rootnoverify (<device-type><device-number>,<partition>)` — Konfiguriert die Root-Partition für GRUB, wie der `root` Befehl, aber mountet die Partition nicht.

Es sind auch andere Befehle verfügbar; geben Sie `info grub` ein, um eine komplette Liste der Befehel zu erhalten. Für eine Beschreibung aller GRUB-Befehle siehe Online-Informationen unter http://www.gnu.org/manual/grub/.

2.7. Menükonfigurationsdatei von GRUB

Die Konfigurationsdatei (`/boot/grub/grub.conf`), die verwendet wird, um die Liste der zu bootenden Betriebssysteme in der Menüoberfläche von GRUB zu erstellen, ermöglicht dem Benutzer im Wesentlichen, eine festgelegte Reihe von Befehlen auszuwählen. Dabei können die in Abschnitt 2.6 angeführten Befehle sowie einige spezielle Befehle verwendet werden, die ausschließlich in der Konfigurationsdatei zur Verfügung stehen.

2.7.1. Struktur der Konfigurationsdatei

Die Konfigurationsdatei der Menüoberfläche von GRUB ist `/boot/grub/grub.conf`. Die Befehle für das Festlegen der allgemeinen Einstellungen für die Menüoberfläche werden am oberen Ende der Datei platziert. Darauf folgen die verschiedenen Einträge für jedes der im Menü genannten Betriebssysteme oder Kernel.

Im Folgenden eine sehr einfache GRUB-Menükonfigurationsdatei, die entweder Red Hat Enterprise Linux oder Microsoft Windows 2000 bootet:

```
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz

# section to load Linux
title Red Hat Enterprise Linux (2.4.21-1.ent)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-1 ro root=/dev/sda2
        initrd /initrd-2.4.21-1.img

# section to load Windows
title Windows
        rootnoverify (hd0,0)
        chainloader +1
```

Diese Datei weist GRUB an, ein Menü mit Red Hat Enterprise Linux als standardmäßigem Betriebssystem zu erstellen, das nach 10 Sekunden automatisch gebootet wird. Gegeben sind zwei Abschnitte - einer pro Betriebssystemeintrag - mit spezifischen Befehlen für die Partitionstabelle der Systemplatte.

Anmerkung

Beachten Sie, dass der Standardwert als Ganzzahl angegeben ist, die sich auf die erste `title`-Zeile in der GRUB-Konfigurationsdatei bezieht.Wenn Sie `windows` im vorigen Beispiel als Standard festlegen möchten, ändern Sie `default=0` zu `default=1`.

Die Konfiguration einer GRUB-Menükonfigurationsdatei für das Starten mehrerer Betriebssysteme übersteigt den Rahmen dieses Kapitels. Siehe Abschnitt 2.11 für eine Liste zusätzlicher Informationsquellen.

2.7.2. Anweisungen für die Konfigurationsdatei

Die folgenden Anweisungen werden häufig in der Menükonfigurationsdatei von GRUB verwendet:

- `chainloader` *</path/to/file>* — Lädt die angegebene Datei als Kettenloader. Ersetzen Sie *</path/to/file>* mit dem absoluten Pfad zum Kettenloader. Wenn sich die Datei auf dem ersten Sektor der festgelegten Partition befindet, verwenden Sie die Blocklisten-Notation `+1`.

- `color <normal-color> < selected color>` — Ermöglicht, spezifische Farben für das Menü einzustellen, wobei zwei Farben als Vorder- und Hintergrundfarben konfiguriert werden. Verwenden Sie einfache Farbbezeichnungen wie `red/black`. Zum Beispiel:
  ```
  color red/black green/blue
  ```
- `default=<integer>` — Ersetzen Sie `<integer>` mit der standardmäßigen Eingabe-Titelnummer, die geladenwerden soll, wenn die Menüoberfläche wegen Zeitüberschreitung abbricht.
- `fallback=<integer>` — Ersetzen Sie `<integer>` mit der Eingabe- Titelnummer für einen erneuten Versuch, wenn der erste Versuch gescheitert ist.
- `hiddenmenu` — Verhindert, dass die GRUB-Menüoberfläche angezeigt wird und lädt den `default` Eintrag, wenn der `timeout`-Zeitraum abläuft. Der Benutzer kann das standardmäßige GRUB-Menü aufrufen, indem er die Taste [Esc] drückt.
- `initrd </path/to/initrd>` — Ermöglicht die Angabe einer initialen RAM-Disk, die beim Booten verwendet wird. Ersetzen Sie `</path/to/initrd>` mit dem absoluten Pfad zu dem ursprünglichen RAM-Speicher.
- `kernel </path/to/kernel> <option-1> <option-N>` — Legt die Kernel-Datei an, die beim Hochfahren des Operationssystems geladen wird. Ersetzen Sie `</path/to/kernel>` mit einem absoluten Pfad von der Partition, die durch den Root-Befehl festgelegt wurde. Mehrere Optionen können an den Kernel weitergegeben werden, wenn er geladen wird.
- `password=<password>` — Verhindert, dass ein Benutzer ohne Passwort die Einträge dieser Menüoption verändert.

  Nach dem Befehl `password <passwort>` können Sie auch eine alternative Menükonfigurationsdatei angeben. In diesem Fall startet GRUB die zweite Stufe des Bootloaders erneut und verwendet diese alternative Konfigurationsdatei,um das Menü zu erstellen. Wenn eine alternative Datei zur Konfiguration des Menüs nicht in den Befehl eingeschlossen wird, dann kann ein Benutzer, der das Passwort kennt, die aktuelle Konfigurationsdatei bearbeiten.

  Für weitere Informationen über die Sicherung von GRUB siehe Kapitel *Workstation Security* im *Red Hat Enterprise Linux Sicherheitshandbuch*.
- `root (<device-type><device-number>,<partition>)` — Konfiguriert die Root-Partition für GRUB, z.B. `(hd0,0)` und mountet die Partition.
- `rootnoverify (<device-type><device-number>,<partition>)` — Konfiguriert die Root-Partition für GRUB, wie der `root` Befehl, aber mountet die Partition nicht.
- `timeout=<integer>` — Legt den Intervall in Sekunden fest, der verstreicht, bevor GRUB die in `default` command enthaltene Eingabe lädt.
- `splashimage=<path-to-image>` — Gibt den Speicherort des Splashscreen-Images an, das verwendet wird, wenn GRUB bootet.
- `title group-title` — Legt einen Titel fest, der einer bestimmten Gruppe von Befehlen zugeordnet ist, die für das Laden eines Kernel oder Betriebssystems benutzt werden.

Um für Benutzer lesbare Kommentare zur Menü-Konfigurationsdatei hinzuzufügen, beginnen Sie die Zeile mit dem Raute-Zeichen (`#`).

2.8. LILO

LILO ist das Akronym für *LI*nux *LO*ader und wurde während vieler Jahre verwendet, um Linux auf x86- Systemen zu starten. Obwohl GRUB jetzt der Standardbootloader ist, bevorzugen manche Personen LILO, da sie mit dem Programm vertraut sind. Andere wiederum verwenden ihn, weil GRUB möglicherweise beim Starten gewisser Hardware Probleme bereitet.

2.8.1. LILO und der x86-Bootprozess

In diesem Abschnitt wird die spezifische Rolle von LILO beim Booten eines x86-Systems ausführlich beschrieben. Detaillierte Informationen zum gesamten Bootprozess finden Sie unter Abschnitt 1.2.

LILO wird fast genauso wie GRUB in den Speicher geladen, mit dem Unterschied, dass es nur ein zweistufiger Loader ist.

1. *Der Stage 1 oder primäre Bootloader wird vom BIOS aus dem MBR in den Speicher gelesen*[2]. Der primäre Bootloader nimmt weniger als 512 Bytes Plattenplatz im MBR in Anspruch. Seine einzige Aufgabe ist das Laden des Stage 2 Bootloaders sowie das Übergeben der Geometriedaten der Platte an ihn.
2. *Der Stage 2- oder sekundäre Bootloader wird in den Speicher gelesen.* Der sekundäre Bootloader zeigt den Red Hat Enterprise Linux Einstiegsbildschirm an. Mit diesem Bildschirm können Sie das Betriebssystem bzw. den Linux-Kernel auswählen, das/der gestartet werden soll.
3. *Der Stage 2 Bootloader liest das Betriebssystem bzw. den Kernel und* `initrd` *in den Speicher.* Sobald LILO festlegt, welches Betriebssystem gestartet werden soll, lädt er es in den Speicher und übergibt die Steuerung des Rechners an das Betriebssystem.

Wenn der Stage 2 Bootloader in den Arbeitsspeicher geladen ist, zeigt LILO den Red Hat Enterprise Linux-Einstiegsbildschirm mit den verschiedenen Betriebssystemen oder Kerneln an, die zum Starten konfiguriert wurden. Wenn Sie standardmäßig nur Red Hat Enterprise Linux installiert haben, ist nur `linux` als Option vorhanden. Sollte das System mehrere Prozessoren haben, wird eine `linux-up` Option für den Einzelprozessor Kernel und eine `linux` Option für den SMP Kernel erscheinen. Ist LILO dazu konfiguriert, andere Betriebssysteme zu booten, erscheinen diese Bootoptionen ebenfalls auf dem Bildschirm.

Die Pfeiltasten ermöglichen Ihnen das Betriebssystem zu markieren, und durch Drücken der [Enter-Taste] wird der Bootvorgang gestartet.

Um Zugriff zu einem `boot:` Prompt zu erhalten, drücken Sie [Strg]-[X].

2.8.2. LILO vs. GRUB

Im Großen und Ganzen gesehen funktioniert LILO wie GRUB, mit Ausnahme folgender drei Hauptunterschiede:

- Die Befehlsoberfläche ist nicht interaktiv.
- Er speichert Informationen über den Speicherort des Kernels oder anderer zu ladenden Betriebssysteme im MBR.
- Er kann keine ext2-Partitionen lesen.

Der erste Punkt bedeutet, dass der Befehls-Prompt für LILO nicht interaktiv ist und nur Befehle mit Argumenten zulässt.

Die letzten beiden Punkte bedeuten, dass Sie nach Änderungen an der Konfigurationsdatei von LILO oder der Installation eines neuen Kernels LILO auf dem MBR neu installieren müssen. Dazu dient der folgende Befehl:

```
/sbin/lilo -v -v
```

Diese Methode stellt ein größeres Risiko als die GRUB-Methode dar, da ein nicht richtig konfigurierter MBR zur Folge hat, dass das System nicht mehr booten kann. Sollte bei GRUB die Konfigurationsdatei fehlerhaft konfiguriert sein, so startet er einfach nur die Befehlszeilenoberfläche, wo der

2. Weitere Informationen zum BIOS und MBR finden Sie unter Abschnitt 1.2.1.

Benutzer das System manuell booten kann. Siehe Abschnitt 2.5 für weitere Informationen zur GRUB Befehlszeilenoberfläche.

Tipp

Wenn Sie den Kernel mit Hilfe von **Red Hat Update Agent** aktualisieren, wird der MBR automatisch aktualisiert. Weitere Informationen zu RHN finden Sie online unter https://rhn.redhat.com

2.9. Die LILO Konfigurationsdatei

Die LILO Konfigurationsdatei heisst `/etc/lilo.conf`. Der Befehl `/sbin/lilo` benutzt diese, um zu bestimmen, welche Information zum MBR geschrieben werden sollen.

Warnung

Wenn Sie Änderungen an `/etc/lilo.conf` vornehmen wollen, sollten Sie unbedingt eine Sicherungskopie der Datei anlegen. Stellen Sie außerdem sicher, dass Sie über eine funktionierende Bootdiskette verfügen, um bei Problemen das System starten und den MBR ändern zu können. Weitere Informationen zum Erstellen einer Bootdiskette finden Sie unter den man-Seiten zu `mkbootdisk`.

Die Datei `/etc/lilo.conf` wird vom Befehl `/sbin/lilo` verwendet, um festzulegen, welches Betriebssystem oder welcher Kernel gestartet wird, wie auch um den eigenen Installationsort zu ermitteln.

2.9.1. Probe `/etc/lilo.conf`

Im Folgenden finden Sie eine Probe `/etc/lilo.conf` für ein System, das so konfiguriert ist, dass es zwei Betriebssysteme hochfahren kann, Red Hat Enterprise Linux und DOS:

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
timeout=50
message=/boot/message
lba32
default=linux

image=/boot/vmlinuz-2.4.0-0.43.6
 label=linux
 initrd=/boot/initrd-2.4.0-0.43.6.img
 read-only
 root=/dev/hda5

other=/dev/hda1
 label=dos
```

Hier ein ausführlicher Blick auf die Zeilen dieser Datei:

- `boot=/dev/hda` — Weist LILO an, sich selbst auf der ersten Festplatte des ersten IDE-Controllers zu installieren.
- `map=/boot/map` — Sucht die Zuordnungsdatei. Normalerweise sollten hier keine Änderungen vorgenommen werden.
- `install=/boot/boot.b` — Weist LILO an, die angegebene Datei als neuen Bootsektor zu installieren. Normalerweise sollten hier keine Änderungen vorgenommen werden. Wenn die `install`-Zeile fehlt, geht LILO davon aus, dass `/boot/boot.b` standardmäßig zu verwenden ist.
- `prompt` — Weist LILO an, alle Verweise in der `message`-Zeile anzuzeigen. Es wird davon abgeraten, die `prompt`-Zeile zu entfernen. Wenn Sie dies dennoch tun, können Sie nach wie vor einen Prompt aufrufen, indem Sie die [Umschalt]-Taste gedrückt halten, während der Rechner hochfährt.
- `timeout=50` — Legt den Zeitraum fest, den LILO auf Benutzereingaben wartet, ehe er mit dem Starten des `default`-Zeileneintrags fortfährt. Dies wird in Zehntelsekunden gemessen. 50 ist der Standardwert.
- `message=/boot/message` — Verweist auf den Bildschirm von LILO, auf dem Sie das zu startende Betriebssystem bzw. den Kernel auswählen.
- `lba32` — Beschreibt LILO die Festplattengeometrie. Ein anderer üblicher Eintrag ist `linear`. Sie sollten diese Zeile nicht ändern, es sei denn, Sie verfügen über die notwendigen Kenntnisse. Ansonsten könnten Sie Ihr System in einen nicht mehr startfähigen Status versetzen.
- `default=linux` — Verweist auf das Betriebssystem, das LILO standardmäßig aus den unterhalb dieser Zeile genannten Optionen starten soll. Der Name `linux` bezieht sich auf die untere Zeile `label` in allen Bootoptionen.
- `image=/boot/vmlinuz-2.4.0-0.43.6` — Gibt den Linux-Kernel an, der mit genau diesen Bootoptionen gestartet werden soll.
- `label=linux` — Benennt die Betriebssystemoption im LILO-Bildschirm. In diesem Fall handelt es sich auch um den Namen, auf den die Zeile `default` verweist.
- `initrd=/boot/initrd-2.4.0-0.43.6.img` — Verweist auf das `initiale RAM-Disk`-Image, das zum Zeitpunkt des Bootens verwendet wird, um die Geräte wirklich zu initialisieren und zu starten, die das Booten des Kernels ermöglichen. Die initiale RAM-Disk ist eine Sammlung von rechnerspezifischen Treibern, die zum Betreiben von SCSI- Karten, Festplatten oder anderer Geräte benötigt wird, die zum Laden des Kernels erforderlich sind. Versuchen Sie niemals, initiale RAM-Disks auf mehreren Rechnern gemeinsam zu nutzen.
- `read-only` — Gibt an, dass die root-Partition (siehe die Zeile `root` unten) schreibgeschützt ist und während des Bootprozesses nicht geändert werden kann.
- `root=/dev/hda5` — Weist LILO an, welche Plattenpartition als root-Partition verwendet werden soll.
- `other=/dev/hda1` — Legt die Partition fest, die DOS enthält.

2.10. Ändern von Runleveln zum Zeitpunkt des Bootens

Unter Red Hat Enterprise Linux können Sie den Standard-Runlevel zum Zeitpunkt des Bootens verändern.

Wenn Sie LILO verwenden, greifen Sie auf den Prompt `boot:` zu, indem Sie die Tasten [Strg]-[X] drücken. Geben Sie anschließend Folgendes ein:

`linux <`*`runlevel-number`*`>`

Ersetzen Sie in diesem Befehl <*Runlevel-Nummer*> entweder durch die Nummer des Runlevels, in dem Sie booten möchten (**1** bis **5**), oder durch das Wort **`single`** oder **`emergency`**.

Falls Sie GRUB verwenden, führen Sie diese Schritte aus:

- Wählen Sie auf dem grafischen GRUB-Bootloader-Bildschirm das **Red Hat Enterprise Linux**-Bootlabel aus und drücken Sie [e], um es zu bearbeiten.
- Gehen Sie mit der Pfeiltaste zur Kernelzeile hinunter und drücken zur Bearbeitung [e].
- Geben Sie am Prompt die Nummer des Runlevels, auf dem Sie booten möchten (**1** bis **5**), das Wort **single** oder **emergency** ein, und drücken Sie dann die [Enter-Taste].
- Sie kehren nun zum GRUB-Bildschirm mit den Kernel-Informationen zurück. Drücken Sie die [b]-Taste, um das System zu starten.

Weitere Informationen über Runlevel finden Sie unter Abschnitt 1.4.1.

2.11. Zusätzliche Ressourcen

Dieses Kapitel stellt lediglich eine Einführung in GRUB und LILO dar. Weitere Informationen über die Funktionsweise von GRUB und LILO finden Sie in folgenden Ressourcen.

2.11.1. Installierte Dokumentation

- `/usr/share/doc/grub-<version-number>/` — Dieses Verzeichnis enthält wertvolle Informationen über die Verwendung und Konfiguration von GRUB. *<version-number>* bezieht sich auf die Version des installierten GRUB Paketes.
- Mit dem Befehl `info grub` können Sie die GRUB Informationsseite aufrufen. Sie enthält eine Einführung, ein Referenzhandbuch für Benutzer, ein Referenzhandbuch für Programmierer sowie ein FAQ-Dokument zu GRUB und seiner Verwendung.
- `/usr/share/doc/lilo-<version-number>/` — Dieses Verzeichnis enthält viele Informationen über die Verwendung und Konfiguration von LILO. Besondere Aufmerksamkeit verdient das Unterverzeichnis `doc/` mit der informativen Postscriptdatei `User_Guide.ps`. *<version-number>* bezieht sich auf die Version des installierten LILO Pakets.

2.11.2. Hilfreiche Websites

- http://www.gnu.org/software/grub — Die Homepage des GNU-GRUB-Projekts. Hier sind Informationen über die Entwicklung von GRUB und ein FAQ-Dokument enthalten.
- http://www.uruk.org/orig-grub — Die ursprüngliche GRUB-Dokumentation, bevor das Projekt zur weiteren Entwicklung an die Free Software Foundation übergeben wurde.
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Multiboot-with-GRUB.html — Behandelt verschiedene Verwendungen für GRUB, einschließlich das Booten von nicht-Linux-Betriebssystemen.
- http://www.linuxgazette.com/issue64/kohli.html — Eine Einführung über die Konfiguration von GRUB auf einem System und ein Überblick der Befehlszeilenoptionen von GRUB.
- http://www.tldp.org/HOWTO/mini/LILO.html — In diesem mini-HOWTO werden die verschiedenen Verwendungsweisen von LILO besprochen, u.a. das Booten von nicht-Linux-Betriebssystemen.

2.11.3. Bücher zu diesem Thema

- *Red Hat Enterprise Linux Sicherheitshandbuch*; Red Hat, Inc. — Das *Workstation Security* Kapitel erklärt in knapper Weise, wie man die GRUB und LILO sichern kann.

redhat.

Kapitel 3.

Struktur des Dateisystems

3.1. Warum eine gemeinsame Struktur?

Die Struktur des Dateisystems ist die niedrigste organisatorische Stufe eines Betriebssystems. Fast alle Wege, mit denen ein Betriebssystem mit seinen Benutzern, seinen Anwendungen und seinem Sicherheitskonzept interagiert, hängen davon ab, wie es Dateien auf Speicherelementen speichert. Das Bereitstellen einer gemeinsamen Struktur des Dateisystems stellt sicher, dass Benutzer und Programme imstande sind, Dateien zu öffnen und Dateien zu schreiben.

Dateisysteme unterteilen Dateien in zwei logische Kategorien:

- Gemeinsam genutzte und nicht gemeinsam genutzte Dateien
- Variable und statische Dateien

gemeinsam genutzte Dateien sind Dateien, auf die lokal zugegriffen werden kann und auf die verschiedene Hosts zugreifen können, während *nicht gemeinsam genutzte* Dateien nur lokalen Hosts zur Verfügung stehen. *Variable* Dateien, wie z.B. Dokumente, können jederzeit geändert werden; *statische* Dateien, wie Binärdateien bleiben ohne Aktion des Systemadministrators unverändert.

Diese Betrachtungsweise soll helfen, die Zusammenhänge zwischen Dateien und den Zugriffsoptionen ihrer Verzeichnisse besser zu erkennen. Die Art, wie das Betriebssystem und seine Benutzer die Dateien verwenden, bestimmt somit auch das Verzeichnis, in dem sie abgelegt werden. Und ob dieses Verzeichnis schreibgeschützt gemountet wird, oder mit Schreib- und Lesezugriff, und welche Zugriffsrechte jeder Benutzer für seine Dateien hat. Ausschlaggebend ist die oberste Organisationsstufe, da der Zugriff auf die darunterliegenden Verzeichnisse eingeschränkt werden kann bzw. sich unter Umständen Sicherheitsprobleme ergeben, wenn die Organisation nicht von oben bis unten einer strengen Struktur unterliegt.

3.2. Übersicht über den Dateisystem-Hierarchiestandard (FHS)

Red Hat benützt die *Filesystem Hierarchy Standard* (*FHS*)-Dateisystemstruktur, die die Namen, Orte und Genehmigungen für viele Dataiarten und Verzeichnisse definiert.

Das aktuelle FHS-Dokument ist die maßgebende Referenz für alle FHS-konformen Dateisystem, wobei der Standard jedoch viele Bereiche undefiniert oder erweiterbar lässt. In diesem Abschnitt geben wir Ihnen einen Überblick über diesen Standard und eine Beschreibung jener Bereiche des Dateisystems, die vom Standard nicht erfasst werden.

Die Erfüllung dieses Standards bedeutet viel, aber die beiden wichtigsten Aspekte sind sicherlich die Kompatibilität mit anderen Systemen und die Möglichkeit, eine `/usr/`-Partition schreibgeschützt zu mounten, weil sie gemeinsam genutzte ausführbare Dateien enthält und daher keine Änderungen durch den Benutzer vorgenommen werden sollten. Da `/usr/` schreibgeschützt gemountet ist, besteht die Möglichkeit, sie über die CD-ROM oder über einen schreibgeschützten NFS-Mount von einem anderen Rechner aus zu mounten.

3.2.1. FHS-Organisation

Die hier beschriebenen Verzeichnisse und Dateien stellen nur eine kleine Teilmenge der im Dokument zum Dateisystemstandard angegebenen Verzeichnisse und Dateien dar. Vollständige Informationen finden Sie im neuesten Dokument zum Dateisystemstandard FHS.

Der vollständige Standard ist online verfügbar unter: http://www.pathname.com/fhs/.

3.2.1.1. Das `/boot/`-Verzeichnis

Das `/boot/`-Verzeichnis enthält statische Dateien, die erforderlich sind, um das System hochzufahren, den Linux Kernel. Diese Dateien sind notwendig, damit das System fehlerfrei hochfahren kann.

Warnung

Entfernen Sie unter keinen Umständen das `/boot/`- Verzeichnis. Wenn Sie dieses Verzeichnis löschen, kann Ihr System nicht mehr gestartet werden.

3.2.1.2. Das `/dev/`-Verzeichnis

Das `/dev/`-Verzeichnis enthält Dateisystemeinträge, die die an das System angeschlossenen Geräte wiedergeben. Diese Dateien sind für das einwandfreie Funktionieren des Systems unerlässlich.

3.2.1.3. Das `/etc/`-Verzeichnis

Das `/etc/`-Verzeichnis ist für lokale Konfigurationsdateien Ihres Rechners reserviert. Unter `/etc/` dürfen keine Binärdateien abgelegt werden. Sämtliche Binärdateien, die zu einem früheren Zeitpunkt in `/etc/` abgelegt wurden, müssen nun nach `/sbin/` oder `/bin/` verschoben werden.

Die Verzeichnisse `X11/` und `skel/` sind Unterverzeichnisse von `/etc/`:

```
/etc
  |- X11/
  |- skel/
```

Im `/etc/X11/`-Verzeichnis werden X Window System-Konfigurationsdateien, wie z.B. `XF86Config`, abgelegt. Im `/etc/skel/`-Verzeichnis werden "skeleton" Benutzerdateien abgelegt. Wenn ein neuer Benutzer hinzukommt, dienen sie dazu, ein Home-Verzeichnis anzulegen.

3.2.1.4. Das `/lib/`-Verzeichnis

Das `/lib/`-Verzeichnis sollte nur jene Bibliotheken enthalten, die für das Ausführen der Binärdateien von `/bin/` und `/sbin/` gebraucht werden. Diese gemeinsam genutzten Bibliothek-Images sind insbesondere für das Hochfahren des Systems und das Ausführen von Befehlen innerhalb des root-Dateisystems von Bedeutung.

3.2.1.5. Das `/mnt/`-Verzeichnis

Das `/mnt/`-Verzeichnis ist für vorübergehend gemountete Dateisysteme, wie CD-ROMs und 3,5 Disketten.

3.2.1.6. Das /opt/-Verzeichnis

Das /opt/-Verzeichnis stellt einen Bereich für die Speicherung von großen und statischen Software-Paketen zur Verfügung.

Für Pakete, deren Dateien nicht über das ganze Dateiystem verteilt abgelegt werden sollen, stellt das /opt/-Verzeichnis ein logisches und überschaubares organisatorisches System mit dem Namen des Pakets zur Verfügung. Der Systemadministrator kann so die Rolle jeder Datei innerhalb eines bestimmten Pakets bestimmen.

Wenn z.B. ein besimmtes Softwarepaket, das in /opt/ abgelegt ist, sample heißt, dann können alle zugehörigen Dateien in Verzeichnisse innerhalb /opt/sample/ abgelegt werden, z.B. /opt/sample/bin/ für Binärdateien und /opt/sample/man/ für manuelle Seiten.

Große Pakete, die zahlreiche Unterpakete umfassen, die jeweils verschiedene Aufgaben erfüllen, werden in /opt/ positioniert, so dass das große Paket eine Organisationsstruktur erhält. Das sample-Paket kann auf diese Weise verschiedene Tools in eigenen Unterverzeichnissen besitzen - beispielsweise /opt/sample/tool1/ und /opt/sample/tool2/, die wiederum ihre eigenen Verzeichnisse wie bin/ oder man/ u.ä. aufweisen.

3.2.1.7. Das /proc/-Verzeichnis

Das /proc/-Verzeichnis enthält spezielle Dateien, die entweder Informationen zum Kernel schicken oder sie vom Kernel erhalten.

Aufgrund der großen Anzahl verfügbarer Daten in /proc/ und der vielen Verwendungsmöglichkeiten dieses Verzeichnisses im Zusammenhang mit dem Kernel, wurde diesem Thema ein ganzes Kapitel gewidmet. Weitere Informationen hierzu finden Sie unter Kapitel 5.

3.2.1.8. Das /sbin/-Verzeichnis

Das /sbin/-Verzeichnis enthält die ausführbaren Dateien, die vom root-Benutzer benützt werden. Die ausführbaren Dateien in /sbin/ dienen ausschließlich dem Hochfahren und führen Wiederherstellungsvorgänge durch. In diesem Verzeichnis bedeutet FHS:

> /sbin/ enthält Binärdateien, die für das Hochfahren, Wiederherstellen, Retten und/oder Reparieren des Systems notwendig sind, sowie Binärdateien in/bin/. Jede nach dem Mounten von /usr/ verwendete ausführbare Datei (sofern keine Probleme auftreten) sollte in /usr/sbin/ abgelegt werden. Lokale Systemverwaltungs-Binärdateien sollten in /usr/local/sbin/.

abgelegt werden.

Zumindest die folgenden Programme sollten sich also in /sbin/ befinden:

```
arp, clock,
halt, init,
fsck.*, grub
ifconfig, lilo,
mingetty, mkfs.*,
mkswap, reboot,
route, shutdown,
swapoff, swapon
```

3.2.1.9. Das /usr/-Verzeichnis

Im /usr/-Verzeichnis werden Dateien abgelegt, die allen Maschinen zur Verfügung gestellt werden. Das /usr/-Verzeichnis liegt oftmals in seiner eigenen Partition und ist schreibgeschützt gemounted. Zumindest folgende Verzeichnisse sollten Unterverzeichnisse von /usr/ sein:

```
/usr
  |- bin/
  |- dict/
  |- doc/
  |- etc/
  |- games/
  |- include/
  |- kerberos/
  |- lib/
  |- libexec/
  |- local/
  |- sbin/
  |- share/
  |- src/
  |- tmp -> ../var/tmp/
  |- X11R6/
```

Im `/usr/` Verzeichnis enthält das `bin/`- Verzeichnis ausführbare Dateien, `dict/` enthält nicht FHS-konforme Dokumentationsseiten, `etc/` enthält Konfigurationsdateien für das gesamte System, `games/` ist für Spiele reserviert, `include/` enthält C-Header-Dateien, `kerberos/` enthält Binärdateien und andere Dateien im Zusammenhang mit Kerberos und `lib/` enthält Objektdateien und Bibliotheken,die nicht konzipiert wurden, um direkt von Benutzern oder Shell-Skripts verwendet zu werden. Das `libexec/`- Verzeichnis enthält kleinere Hilfsprogramme, die von anderen Programmen aufgerufen werden, `sbin/` enthält die Binärdateien für die Systemverwaltung (jene Binärdateien, die nicht zu `/sbin/`) gehören), `share/` enthält Dateien, die nicht architekturspezifisch sind, `src/` ist für den Quellcode reserviert und `X11R6/` ist für das X-Window-System gedacht. (XFree86 auf Red Hat Enterprise Linux).

3.2.1.10. Das `/usr/local/`-Verzeichnis

Laut FHS:

> "Die `/usr/local/`-Hierarchie kann vom Systemadministrator für die Installation lokaler Software benutzt werden. Bei der Aktualisierung der Systemsoftware muss ein Überschreiben ausgeschlossen werden. Das Verzeichnis kann für Programme und Daten benutzt werden, auf die innerhalb einer Gruppe von Rechnern zugegriffen werden kann, und die nicht in `/usr/` abgelegt sind."

Das `/usr/local/`-Verzeichnis hat eine ähnliche Struktur wie das `/usr/`-Verzeichnis. Es enthält die folgenden Unterverzeichnisse, deren Verwendungszweck jeweils dem der Unterverzeichnisse im `/usr/`-Verzeichnis ähnlich ist:

```
/usr/local
       |- bin/
       |- doc/
       |- etc/
       |- games/
       |- include/
       |- lib/
       |- libexec/
       |- sbin/
       |- share/
       |- src/
```

In Red Hat Enterprise Linux unterscheidet sich der Verwendungszweck für `/usr/local/` leicht von den durch FHS definierten Verwendungszwecken. Laut FHS soll `/usr/local/` bei jener Software abgelegt werden, die vor Aktualisierungen der System-Software geschützt bleiben soll. Da Software-

Aktualisierungen sicher mit *Red Hat Package Manager* (*RPM*) durchgeführt werden können, ist es nicht notwendig, Dateien zu schützen, indem sie in `/usr/local/` abgelegt werden.Stattdessen empfehlen wir Ihnen, für lokal auf Ihrem Rechner verwendete Software auf `/usr/local/` zurückzugreifen.

Wenn, zum Beispiel, das Verzeichnis `/usr/` als eine Read-Only (Nur-Lesen) NFS Share von einem Remote Host gemountet wird, ist es immernoch möglich, ein Programm oder Paket unter `/usr/local/` zu installieren.

3.2.1.11. Das `/var/`-Verzeichnis

Der Dateisystemstandard FHS erfordert, dass das Mounten von `/usr/` im schreibgeschützten Modus möglich ist. Daher sollten Programme, die Protokolldateien schreiben oder `spool/` oder `lock/`-Verzeichnisse benötigen, am besten in das`/var/` Verzeichnis schreiben. Laut FHS steht `/var/` für:

> "...variable Datendateien. Dazu gehören Spool-Verzeichnisse und Spooldateien, Systemverwaltungs- und Protokollierungsdaten sowie zwischengespeicherte Dateien."

Nachfolgend einige der Verzeichnisse, die im `/var/` Verzeichnis gefunden werden können:

```
/var
  |- account/
  |- arpwatch/
  |- cache/
  |- crash/
  |- db/
  |- empty/
  |- ftp/
  |- gdm/
  |- kerberos/
  |- lib/
  |- local/
  |- lock/
  |- log/
  |- mail -> spool/mail/
  |- mailman/
  |- named/
  |- nis/
  |- opt/
  |- preserve/
  |- run/
  +- spool/
       |- at/
       |- clientmqueue/
       |- cron/
       |- cups/
       |- lpd/
       |- mail/
       |- mqueue/
       |- news/
       |- postfix/
       |- repackage/
       |- rwho/
       |- samba/
       |- squid/
       |- squirrelmail/
       |- up2date/
```

```
      |- uucppublic/
      |- vbox/
|- tmp/
|- tux/
|- www/
|- yp/
```

Systemprotokolldateien wie z.B. `messages` und `lastlog` werden im `/var/log/`- Verzeichnis abgelegt. Das `/var/lib/rpm/`-Verzeichnis enthält auch die RPM- Systemdatenbanken. Sperrdateien werden in `/var/lock/`, abgelegt, wobei es sich hier normalerweise um spezifische Verzeichnisse für das Programm handelt, das diese Dateien benutzt. Das `/var/spool/`-Verzeichnis hat Unterverzeichnisse für Programme, in denen Datendateien gespeichert werden..

3.3. Spezielle Dateispeicherstellen unter Red Hat Enterprise Linux

Red Hat Enterprise Linux erweitert die FHS-Struktur ein wenig, um Platz für spezielle Dateien zu schaffen.

Die meisten Dateien, die zum RPM gehören, werden im Verzeichnis `/var/lib/rpm/` hinterlegt. Weitere Informationen über RPM finden Sie im Kapitel *Paketverwaltung mit RPM* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Das `/var/spool/up2date/`-Verzeichnis enthält Dateien, die vom **Red Hat Update Agent** verwendet werden, einschließlich RPM-Header-Informationen für das System. Hier können Sie auch RPMs, die Sie während des Updates Ihres Systems heruntergeladen haben, zwischenspeichern. Weitere Informationen zum Red Hat Network finden Sie online unter: https://rhn.redhat.com/.

Eine weitere Red Hat Enterprise Linux-spezifische Speicherstelle ist das `/etc/sysconfig/`-Verzeichnis. In diesem Verzeichnis wird eine ganze Reihe unterschiedlicher Konfigurationsinformationen gespeichert. Viele Skripts, die beim Booten ausgeführt werden, greifen auf die Dateien in diesem Verzeichnis zurück. Siehe hierzu Kapitel 4 für weitere Informationen über den Inhalt dieses Verzeichnisses und die Bedeutung, die diese Dateien für den Bootprozess haben.

Schließlich soll auch das `/initrd/`-Verzeichnis nicht unerwähnt bleiben. Es ist zwar leer, wird aber während des Boot-Prozesses als kritischer Mount-Punkt verwendet.

Warnung

Entfernen Sie unter gar keinen Umständen das `/initrd/`- Verzeichnis. Wenn Sie dieses Verzeichnis löschen, kann Ihr System nicht starten und der Kernel gibt eine gravierende Fehlermeldung aus.

redhat.

Kapitel 4.

Das Verzeichnis `sysconfig`

Das Verzeichnis `/etc/sysconfig/` ist der Ort, an dem eine Vielzahl von Konfigurationsdateien für Red Hat Enterprise Linux aufbewahrt werden.

Dieses Kapitel spricht einige der Dateien im Verzeichnis `/etc/sysconfig/` sowie deren Funktionen und deren Inhalt an. Die Information in diesem Kapitel erhebt keinen Anspruch auf Vollständigkeit, da viele der Dateien eine Reihe von Optionen haben, die nur in sehr spezifischen Fällen verwendet werden.

4.1. Dateien im Verzeichnis `/etc/sysconfig/`

Folgende Dateien befinden sich normalerweise in `/etc/sysconfig/`:

- `amd`
- `apmd`
- `authconfig`
- `clock`
- `desktop`
- `devlabel`
- `dhcpd`
- `firstboot`
- `gpm`
- `harddisks`
- `hwconf`
- `i18n`
- `init`
- `ip6tables-config`
- `iptables-config`
- `irda`
- `keyboard`
- `kudzu`
- `mouse`
- `named`
- `netdump`
- `network`
- `ntpd`
- `pcmcia`
- `radvd`
- `rawdevices`

- redhat-config-securitylevel
- redhat-config-users
- redhat-logviewer
- samba
- sendmail
- spamassassin
- squid
- tux
- vncservers
- xinetd

Anmerkung

Sollten einige dieser Dateien nicht im Verzeichnis /etc/sysconfig/ enthalten sein, sind die entsprechenden Programme eventuell nicht installiert.

Im Folgenden eine Beschreibung dieser Dateien. Dateien, die hier nicht aufgelistet sind sowie extra Dateioptionen können in der /usr/share/doc/initscripts-<*Versionsnummer*>/sysconfig.txt Datei (ersetzen Sie <*Versionsnummer*> mit der Version des initscripts Paketes) gefunden werden. Auch ein Blick in die Initscripts im /etc/rc.d/ Verzeichnis kann hilfreich sein.

4.1.1. /etc/sysconfig/amd

Die Datei /etc/sysconfig/amd enthält verschiedene Parameter, die von amd verwendet werden und das automatische Mounten und Unmounten von Dateisystemen ermöglichen.

4.1.2. /etc/sysconfig/apmd

Die Datei /etc/sysconfig/apmd wird von apmd verwendet, um zu erfahren, welche Prozesse nach den Befehlen suspend/resume gestartet/gestoppt/geändert werden sollen. In ihr ist festgelegt, ob apmd beim Starten aktiviert oder deaktiviert wird, je nachdem ob Ihre Hardware *Advanced Power Management* (*APM*) unterstützt bzw. ob Sie diese Funktionalität benutzen möchten oder nicht. apm ist ein Daemon mit Kontrollfunktion, der im Linux-Kernel mit einem Power-Management-Code arbeitet. Er kann darauf hinweisen, dass die Batterie fast leer ist, falls Sie ein Laptop verwenden, und andere Einstellungen im Bereich Stromversorung.

4.1.3. /etc/sysconfig/authconfig

Die Datei /etc/sysconfig/authconfig legt die Art der Authorisierung fest, die auf dem Rechner verwendet werden soll. Sie enthält mindestens eine der folgenden Zeilen:

- USEMD5=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - yes — MD5 wird zur Authentifizierung verwendet.
  - no — MD5 wird nicht zur Authentifizierung verwendet.

- `USEKERBEROS=<`*`Wert`*`>`, wobei <*`Wert`*> einer der folgenden Werte ist:
  - `yes` — Kerberos wird zur Authentifizierung verwendet.
  - `no` — Kerberos wird nicht zur Authentifizierung verwendet.

- `USELDAPAUTH=<`*`Wert`*`>`, wobei <*`Wert`*> einer der folgenden Werte ist:
  - `yes` — LDAP wird zur Authentifizierung verwendet.
  - `no` — LDAP wird nicht zur Authentifizierung verwendet.

4.1.4. `/etc/sysconfig/clock`

Die Datei `/etc/sysconfig/clock` steuert die Interpretation der Werte der Hardware-System-Uhr.

Derzeit gelten die folgenden Werte:

- `UTC=<`*`Wert`*`>`, wobei <*`Wert`*> einer der folgenden booleschen Werte ist:
  - `true` oder `yes` — Die Hardware-Uhr ist auf UTC (Universal Time Coordinate) eingestellt.
  - `false` oder `no` — Die Hardware-Uhr ist auf lokale Zeit eingestellt.

- `ARC=<`*`Wert`*`>`, wobei <*`Wert`*> einer der folgenden Werte ist:
  - `true` oder `yes` — Zeigt an, dass der 42-Jahre-Offset der Konsole aktiviert ist. Diese Einstellung ist lediglich für ARC- oder AlphaBIOS-basierte Alpha-Systeme. Alle anderen Werte geben an, dass die normale UNIX-Epoche eingestellt ist.

- `SRM=<`*`Wert`*`>`, wobei <*`Wert`*> folgender ist:
  - `true` oder `yes` — Die 1900-Epoche der Konsole ist aktiviert. Diese Einstellung ist lediglich für SRM-basierte Alpha-Systeme. Jeder andere Wert gibt an, dass die normale UNIX-Epoche eingestellt ist.

- `ZONE=<`*`Dateiname`*`>` — Die Zeitzonen-Datei unter `/usr/share/zoneinfo`, von der `/etc/localtime` eine Kopie ist. Diese Datei enthält Informationen wie:
  `ZONE="America/New York"`

Frühere Versionen von Red Hat Linux und Red Hat Enterprise Linux haben folgende Versionen benützt (die nicht länger verwendet werden):

- `CLOCKMODE=<`*`Wert`*`>`, wobei <*`Wert`*> einer der folgenden Werte ist:
  - `GMT` — Zeigt an, dass die Uhr auf Weltzeit (GMT) eingestellt ist.
  - `ARC` — Zeigt an, dass der 42-Jahre-Offset der Konsole aktiviert ist (nur bei Alpha-gestützten Systemen).

4.1.5. /etc/sysconfig/desktop

Die Datei /etc/sysconfig/desktop legt den Desktop für neue Benutzer fest und führt den Display-Manager bei Erreichen von Runleverl 5 aus.

Die richtigen Werte sind:

- DISPLAY=<*value*>, wobei <*value*> einer der folgenden Werte ist:
  - GNOME — Wählt die GNOME Desktop-Umgebung aus.
  - KDE — Wählt die KDE-Desktop-Umgebung aus.

- DISPLAYMANAGER=<*value*>, wobei <*value*> einer der folgenden Werte ist:
  - GDM — Wählt den GNOME Display-Manager aus.
  - KDM — Wählt den KDE-Display-Manager aus.
  - XDM — Wählt den Xfree86 Display-Manager aus.

Mehr über das X Window System unter Red Hat Enterprise Linux erfahren Sie unter Kapitel 7.

4.1.6. /etc/sysconfig/devlabel

Das /etc/sysconfig/devlabel ist die devlabel Konfigurationsdatei. Sie sollte nicht von Hand verändert, sondern mit Hilfe des /sbin/devlabel Befehls konfiguriert werden.

Anweisungen für die Verwendung des devlabel Befehls finden Sie im Kapitel *User-Defined Device Names* in der *Red Hat Enterprise Linux Handbuch zur System-Administration*.

4.1.7. /etc/sysconfig/dhcpd

Die Datei /etc/sysconfig/dhcpd wird verwendet, um beim Booten Argumente an den dhcpd-Daemon zu übertragen. Der dhcpd-Daemon implementiert das Dynamic Host Configuration Protocol (DHCP) und das Internet Bootstrap Protocol (BOOTP). DHCP und BOOTP weisen Rechnern auf dem Netzwerk Hostnamen zu. Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf den man-Seiten von dhcpd.

4.1.8. /etc/sysconfig/firstboot

Ab Red Hat Linux 8.0 ruft das Programm /sbin/init beim Erststart des Systems das Skript etc/rc.d/init.d/firstboot auf. Dieses Skript ruft seinerseits **Setup Agent** auf. Diese Applikation ermöglicht dem Benutzer das Installieren weiterer Anwendungen und Dokumentation vor dem Abschluss des Initialstarts.

Die Datei /etc/sysconfig/firstboot weist den **Setup Agent** einfach an, nicht ausgeführt zu werden. Wenn diese Applikation beim nächsten Systemstart ausführen möchten, müssen Sie einfach nur /etc/sysconfig/firstboot entfernen und chkconfig --level 5 firstboot on ausführen.

4.1.9. /etc/sysconfig/gpm

Die Datei /etc/sysconfig/gpm wird verwendet, um beim Booten Argumente an den gpm-Daemon zu übertragen. Der gpm-Daemon ist der Maus-Server, mit dem die Geschwindigkeit der Maus erhöht und die Möglichkeit des Kopierens mit der mittleren Maus-Taste geschaffen werden kann. Weitere Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf den man-Seiten von gpm. Standardmäßig ist die Maus auf /dev/mouse eingestellt.

4.1.10. /etc/sysconfig/harddisks

Die Datei /etc/sysconfig/harddisks ermöglicht es Ihnen, Ihre Festplatte(n) abzustimmen. Der Administrator kann auch /etc/sysconfig/hardiskhd[a-h] verwenden, um die Parameter für bestimmte Laufwerke zu konfigurieren.

Warnung

Nehmen Sie keine leichtsinnigen Änderungen in dieser Datei vor. Wenn Sie die hier gespeicherten Standardwerte ändern, besteht das Risiko, dass Sie alle Daten der Festplatte(n) verlieren!

Die Datei /etc/sysconfig/harddisks kann Folgendes enthalten:

- USE_DMA=1, wobei der Wert 1 DMA aktiviert. Bei einigen Chipsätzen und Festplattenkombinationen kann DMA jedoch zu Datenverluste verursachen. *Lesen Sie in der Dokumentation Ihrer Festplatte nach oder wenden Sie sich an den Hersteller, bevor Sie diesen Befehl aktivieren.*
- Multiple_IO=16, die Einstellung 16 lässt mehrere Sektoren pro E/A-Interrupt zu. Ist diese Funktion aktiviert, wird der Verwaltungsaufwand des Betriebssystems um 30-50% reduziert. *Äußerste Vorsicht!*
- EIDE_32BIT=3 aktiviert (E)IDE 32-Bit E/A-Support für eine Schnittstellen-Karte.
- LOOKAHEAD=1 aktiviert Lookahead-Lesezugriffe auf das Laufwerk.
- EXTRA_PARAMS= legt fest, wo zusätzliche Parameter hinzugefügt werden können.

4.1.11. /etc/sysconfig/hwconf

In der Datei /etc/sysconfig/hwconfig sind alle Hardware-Komponenten aufgeführt, die kudzu in Ihrem System entdeckt hat, außerdem Informationen zu den verwendeten Treibern, der Anbieter-ID und der Geräte-ID. kudzu findet und konfiguriert neue bzw. geänderte Hardware-Komponenten. Die Datei /etc/sysconfig/hwconfig ist nicht dazu gedacht, manuell bearbeitet zu werden. Wenn Sie sie dennoch bearbeiten, könnte es passieren, dass manche Geräte plötzlich als hinzugefügt oder entfernt angezeigt werden.

4.1.12. /etc/sysconfig/i18n

Mit der Datei /etc/sysconfig/i18n wird die Standardsprache, jede unterstützte Sprache und der Default-System-Font eingestellt. Zum Beispiel:

```
LANG="en_US.UTF-8"
SUPPORTED="en_US.UTF-8:en_US:en"
SYSFONT="latarcyrheb-sun16"
```

4.1.13. /etc/sysconfig/init

In der Datei /etc/sysconfig/init wird das Erscheinungsbild und die Funktion des Systems während des Hochfahrens gesteuert

Folgende Werte können verwendet werden:

- BOOTUP=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - BOOTUP=color stellt die standardmäßige Bildschirmdarstellung beim Systemstart dar, wobei der Erfolg oder Misserfolg von Geräten und Diensten beim Booten in verschiedenen Farben angezeigt wird.
  - BOOTUP=verbose erzeugt ein Display im herkömmlichen Stil. Dieses Display liefert mehr Informationen als bloße Mitteilungen über Erfolg oder Misserfolg.
  - Alle anderen Werte erzeugen ein neues Display, aber ohne ANSI-Formatierung.

- RES_COL=<*Wert*>, wobei <*Wert*> die Spaltennummer des Bildschirms ist, in der Status-Kennungen beginnen. Standardeinstellung ist 60.
- MOVE_TO_COL=<*Wert*>, wobei <*Wert*> den Cursor zu dem Wert in der Zeile RES_COL führt, was über den Befehl echo -en geschieht.
- SETCOLOR_SUCCESS=<*Wert*>, wobei <*Wert*> die Farbe für die Anzeige von erfolgreichen Vorgängen ist. Dies geschieht über den Befehl echo -en, wobei die Farbe auf grün gesetzt wird.
- SETCOLOR_FAILURE=<*Wert*>, wobei <*Wert*> die Farbe für die Anzeige von nicht erfolgreichen Vorgängen bestimmt. Dies geschieht über den Befehl echo -en, wobei die Farbe rot eingestellt wird.
- SETCOLOR_WARNING=<*Wert*>, wobei <*Wert*> die Farbe für die Anzeige von Warnungen bestimmt. Dies geschieht über den Befehl echo -en, wobei die Farbe gelb eingestellt wird.
- SETCOLOR_NORMAL=<*Wert*>, wobei <*Wert*> 'normal' eingestellt wird. Dies geschieht über den Befehl echo -en.
- LOGLEVEL=<*Wert*>, wobei <*Wert*> den anfänglichen Anmelde-Level für den Kernel bestimmt. Die Standardeinstellung ist 3. Der Wert 8 aktiviert alles (einschließlich Debugging), der Wert 1 deaktivert alles außer der Kernel-Panik. syslogd hebt diese Einstellungen auf, nachdem es gestartet ist.
- PROMPT=<*Wert*>, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - yes — Aktiviert die Key-Überprüfung für den interaktiven Modus.
  - no — Deaktiviert die Key-Überprüfung für den interakiven Modus.

4.1.14. /etc/sysconfig/ipt6ables-config

Die /etc/sysconfig/ip6tables Datei speichert vom Kernel verwendete Informationen, um die IPv6 Paketfilterung einzurichten, beim Hochfahren oder immer wenn der ip6tables Dienst gestartet wird.

Verändern Sie diese Datei nicht von Hand, außer Sie sind mit der Konstruktion von ip6tables Regeln vertraut. Die Regeln können mit dem /sbin/ip6tables Befehl auch manuell aufgestellt werden Wenn die Regeln aufgestellt sind fügen Sie sie in die /etc/sysconfig/ip6tables Datei ein, indem Sie den folgenden Befehl eingeben:

```
/sbin/service ip6tables save
```

Once this file exists, any firewall rules saved in it persists through a system reboot or a service restart.

Mehr Information zu ip6tables finden Sie unter Kapitel 15.

4.1.15. /etc/sysconfig/iptables-config

Die /etc/sysconfig/iptables Datei speichert Information, die der Kernel verwendet, um Paketfilterungsdienste einzurichten, entweder beim Hochfahren oder wann immer der Dienst gestartet wird.

Wenn Sie mit der Erstellung der iptables-Regeln noch nicht vertraut sind, sollten Sie diese Datei nicht manuell ändern. Es ist am einfachsten, solche Regeln mit der **Security Level Configuration Tool** (redhat-config-securitylevel) Anwendung zu verwenden und eine Firewall zu errichten. Diese Anwendungen bearbeiten die Datei automatisch am Ende des Prozesses.

Die Regeln können auch manuell erstellt werden, indem der /sbin/iptables Befehl verwendet wird. Sobald die Regeln erstellt wurden, fügen Sie sie zum /etc/sysconfig/iptables hinzu. Geben Sie den folgenden Befehl ein:

```
/sbin/service iptables save
```

Once this file exists, any firewall rules saved in it persists through a system reboot or a service restart.

Mehr Information über iptables finden Sie unter Kapitel 15.

4.1.16. /etc/sysconfig/irda

Die Datei /etc/sysconfig/irda steuert die Konfiguration der Infrarot-Geräte auf Ihrem System beim Starten.

Folgende Werte können verwendet werden:

- IRDA=<*Wert*>, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - yes — irattach wird ausgeführt, wodurch regelmäßig überprüft wird, ob irgendeine Komponente versucht, eine Verbindung zum Infrarot-Port herzustellen, z.B. ein anderes Notebook, das versucht, eine Netzwerkverbindung herzustellen. Damit Infrarot- Geräte auf Ihrem System laufen können, muss diese Zeile auf yes eingestellt sein.
  - no — irattach wird nicht ausgeführt und verhindert daher eine Verbindung zu Infrarot-Geräten.

- DEVICE=<*Wert*>, wobei <*Wert*> das Gerät ist (normalerweise ein serieller Port), über das die Infrarot-Verbindungen abgewickelt werden.
- DONGLE=<*Wert*>, wobei <*Wert*> die Art Dongle angibt, die für die Infrarot-Kommunikation verwendet wird. Diese Einstellung ist für die Benutzer wichtig, die serielle Dongles statt eigentlicher Infrarot-Ports verwenden. Ein Dongle ist ein Gerät, das mit einem herkömmlichen seriellen Port verbunden ist, um per Infrarot zu kommunizieren. Diese wird standardmäßig auskommentiert, da Notebooks mit echten Infrarot-Ports viel häufiger vorkommen als Computer mit angefügten Dongles.
- DISCOVERY=<*Wert*>, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - yes — Startet irattach im Entdeckungs-Modus, d.h. dieser Befehl sucht aktiv nach anderen Infrarot-Geräten. Dieser Befehl muss aktiviert werden, damit der Rechner aktiv nach einer Infrarot-Verbindung suchen kann (d.h. nach dem Peer, der die Verbindung nicht einleitet).
  - no — Startet irattach nicht im Discovery-Modus.

4.1.17. /etc/sysconfig/keyboard

Die Datei /etc/sysconfig/keyboard steuert das Tastatur-Verhalten. Folgende Werte können verwendet werden:

- KEYBOARDTYPE=sun|pc. Wird nur bei Spark-Prozessoren verwendet. sun gibt an, dass eine Sun-Tastatur an /dev/kbd angeschlossen ist, und pc steht für die Verbindung einer PS/2-Tastatur mit einem PS/2-Port.
- KEYTABLE=<*Datei*>, wobei <*Datei*> der Name der keytable-Datei ist.

  Beispiel: KEYTABLE="us". Die Dateien, die als keytables verwendet werden können, beginnen unter /lib/kbd/keymaps/i386 und verzweigen von dort aus in verschiedene Tastatur-Layouts, die alle mit <*Datei*>.kmap.gz gekennzeichnet sind. Die erste Datei, die unter /lib/kbd/keymaps/i386 mit der KEYTABLE-Einstellung übereinstimmt, wird verwendet.

4.1.18. /etc/sysconfig/kudzu

Mit /etc/sysconfig/kuzdu können Sie beim Booten mit Hilfe von kudzu eine sichere Überprüfung Ihrer System-Hardware vornehmen. Bei einer sicheren Überprüfung wird die Überprüfung der seriellen Ports deaktiviert.

- SAFE=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - yes — kuzdu führt eine sichere Überprüfung aus.
  - no — kuzdu führt eine normale Überprüfung aus.

4.1.19. /etc/sysconfig/mouse

Die Datei /etc/sysconfig/mouse stellt Informationen über die verfügbare Maus zur Verfügung. Die folgenden Werte können verwendet werden:

- FULLNAME=<*Wert*>, wobei sich <*Wert*> auf den vollen Namen der verwendeten Mausart bezieht.
- MOUSETYPE=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - imps2 — Generische USB Rad-Maus.
  - microsoft — Microsoft™-Maus.
  - mouseman — MouseMan™-Maus.
  - mousesystems — Mouse Systems™- Maus.
  - ps/2 — PS/2-Maus.
  - msbm — Microsoft™-Bus-Maus.
  - logibm — Logitech™-Bus-Maus
  - atibm — ATI™-Bus-Maus.
  - logitech — Logitech™-Maus.
  - mmseries — ältere MouseMan™- Maus.

  - `mmhittab` — mmhittab-Maus.

- `XEMU3=<`*`Wert`*`>`, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - `yes` — Die Maus hat nur zwei Buttons, drei Buttons sollten jedoch emuliert werden.
  - `no` — Die Maus hat bereits drei Buttons.
- `XMOUSETYPE=<`*`Wert`*`>`, wobei sich <*Wert*> auf die Mausart bezieht, die bei der Ausführung von X verwendet wird. Die hier aufgeführten Optionen entsprechen den `MOUSETYPE`-Einstellungen dieser Datei.
- `DEVICE=<`*`Wert`*`>`, wobei <*Wert*> die Maus ist.

Außerdem gibt es `/dev/mouse`, einen symbolischen Link, der auf das eigentliche Mausgerät zeigt.

4.1.20. `/etc/sysconfig/named`

Die Datei `/etc/sysconfig/named` wird verwendet, um beim Booten Argumente an den `named`-Daemon zu übertragen. Der `named`-Daemon ist ein *Domain Name System* (*DNS*)-Server, der die Version 9 von *Berkeley Internet Name Domain* (*BIND*) implementiert. Auf diesem Server gibt es eine Tabelle, mit deren Hilfe bestimmte Hostnamen IP-Adressen im Netzwerk zugeordnet werden.

Verwenden Sie bitte bis auf weiteres nur die folgenden Werte:

- `ROOTDIR="<`*`/irgend/wo`*`>"`, wobei sich <*/irgend/wo*> auf den vollständigen Verzeichnispfad einer konfigurierten Chroot-Umgebung bezieht, unter der `named` ausgeführt wird. Besagte Umgebung muss zunächst konfiguriert werden. Nach Eingabe von `info chroot` erhalten Sie mehr Informationen dazu, wie Sie bei der Konfiguration vorgehen müssen.
- `OPTIONS="<`*`Wert`*`>"`, wobei <*Wert*> jede der auf der man-Seite für `named` aufgeführten Optionen sein kann, mit Ausnahme von **`-t`**. An Stelle von **`-t`** verwenden Sie oben bitte die `ROOTDIR`-Zeile.

Informationen zu den Parametern, die für diese Datei zur Verfügung stehen, erhalten Sie auf der man-Seite von `named`. Detaillierte Informationen zum Konfigurieren eines BIND-DNS-Servers finden Sie unter Kapitel 11. Standardmäßig enthält diese Datei keine Parameter.

4.1.21. `/etc/sysconfig/netdump`

`/etc/sysconfig/netdump` ist die Konfigurationsdatei für den `/etc/init.d/netdump`- Dienst. Mit dem `netdump`-Dienst werden sowohl Oops- also auch Speicherdaten auf dem Netzwerk übertragen. `netdump` ist grundsätzlich nicht erforderlich. Sie sollten diese Datei also nur ausführen, wenn es unbedingt notwendig ist. Weitere Informationen zu den Parametern, die für diese Datei zur Verfügung stehen, erhalten Sie auf den man-Seiten von `netdump`.

4.1.22. `/etc/sysconfig/network`

Die Datei `/etc/sysconfig/arpwatch` wird verwendet, um Informationen über die gewünschte Netzwerkkonfiguration anzugeben. Die folgenden Werte können verwendet werden:

- `NETWORKING=<`*`Wert`*`>`, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - `yes` — Das Netzwerk sollte konfiguriert sein.
  - `no` — Das Netzwerk sollte nicht konfiguriert sein.

- HOSTNAME=<*Wert*>, wobei <*Wert*> der *Fully Qualified Domain Name* (*FQDN*) sein sollte, z.B. hostname.domain.com, kann aber auch jeder andere, von Ihnen gewünschte Hostname sein.

Anmerkung

Um die Kompatibilität mit älterer Software (z.B.trn) zu gewährleisten, sollte die /etc/HOSTNAME-Datei den gleichen Wert wie hier enthalten.

- GATEWAY=<*Wert*>, wobei <*Wert*> die IP-Adresse des Netzwerk-Gateways ist.
- GATEWAYDEV=<*Wert*>, wobei <*Wert*> das Gateway-Gerät ist, z.B. eth0.
- NISDOMAIN=<*Wert*>, wobei <*Wert*> der NIS-Domainname ist.

4.1.23. /etc/sysconfig/ntpd

Die Datei /etc/sysconfig/ntpd wird verwendet, um beim Booten Argumente an den ntpd-Daemon zu übertragen. Mit dem ntpd-Daemon wird die Systemuhr eingestellt und in Übereinstimmung mit einem Standard-Zeit-Server im Internet gebracht. Hierbei wird Version 4 des Network Time Protocol (NTP) implementiert. Weitere Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie, wenn Sie den Browser zu folgender Datei führen: /usr/share/doc/ntp-<*Version*>/ntpd.htm (wobei <*Version*> die Versionsnummer vonntpd ist). Standardmäßig legt diese Datei den Besitzer des ntpd-Prozesses auf den Benutzer ntp.

4.1.24. /etc/sysconfig/pcmcia

Mit der Datei /etc/sysconfig/pcmcia werden die Informationen zur Konfiguration von PCMCIA bestimmt. Die folgenden Werte können verwendet werden:

- PCMCIA=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - yes — Der PCMCIA-Support sollte aktiviert werden.
  - no — Der PCMCIA-Support sollte nicht aktiviert werden.

- PCIC=<*Wert*>, wobei <*Wert*> einer der folgenden Werte ist:
  - i82365 — Der Computer verfügt über einen Chipsatz mit i82365-PCMCIA-Steckplatz.
  - tcic — Der Computer verfügt über einen Chipsatz mit tcic-PCMCIA-Steckplatz.

- PCIC_OPTS=<*Wert*>, wobei <*Wert*> die Timing-Parameter für den Steckplatztreiber angibt (i82365 oder tcic).
- CORE_OPTS=<*Wert*>, wobei <*Wert*> die Liste der pcmcia_core-Optionen ist.
- CARDMGR_OPTS=<*Wert*>, wobei <*Wert*> die Liste mit den Optionen für den PCMCIA-cardmgr ist (z.B. -q für den Ruhemodus -m, um nach ladbaren Kernelmodulen im angegebenen Verzeichnis zu suchen usw.). Weitere Informationen finden Sie auf der cardmgr-man-Seite.

4.1.25. /etc/sysconfig/radvd

Die Datei /etc/sysconfig/radvd wird verwendet, um beim Booten Argumente an den radvd-Daemon zu übertragen. Der radvd-Daemon hört Router-Anfragen ab und versendet Router-Anzeigen für das IP Version 6-Protokoll. Mit diesem Dienst können die Rechner eines Netzwerks dynamisch ihre Standard-Router auf der Grundlage vorgenannter Router-Anzeigen ändern. Weitere Informationen zu den Parametern, die Sie in dieser Datei benutzen können, erhalten Sie auf den man-Seiten von radvd. Standardmäßig stellt diese Datei als Besitzer des radvd-Prozesses den Benutzer radvd ein.

4.1.26. /etc/sysconfig/rawdevices

Mit der Datei /etc/sysconfig/rawdevices werden Rawdevice-Verbindungen konfiguriert, z.B.:

```
/dev/raw/raw1 /dev/sda1
/dev/raw/raw2 8 5
```

4.1.27. /etc/sysconfig/redhat-config-securitylevel

Die Datei /etc/sysconfig/redhat-config-securitylevel enthält alle Optionen, welche beim letzten Ausführen von **Security Level Configuration Tool** (redhat-config-securitylevel) gewählt wurden. Benutzer sollten diese Datei nicht manuell bearbeiten. Für mehr Informationen zu **Security Level Configuration Tool** lesen Sie das Kapitel *Basiskonfiguration der Firewall* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

4.1.28. /etc/sysconfig/redhat-config-users

Die Datei /etc/sysconfig/redhat-config-users ist die Konfigurationsdatei für die grafische Applikation **User Manager**. Diese Datei dazu verwendet, um Systembenutzer, wie root , daemon, oder lp herauszufiltern. Diese Datei kann über das Pull-Down-Menü **Einstellungen => Systembenutzer und Gruppen filtern** in der Anwendung **User Manager** bearbeitet werden. Die Bearbeitung sollte nicht manuell erfolgen. Weitere Informationen zur Verwendung dieser Anwendung finden Sie im Kapitel *Benutzer- und Gruppen-Konfiguration* des *Red Hat Enterprise Linux Handbuch zur System-Administration*.

4.1.29. /etc/sysconfig/redhat-logviewer

Die Datei /etc/sysconfig/redhat-logviewer ist die Konfigurationsdatei für die grafische interaktive Anwendung zum Anzeigen von Protokollen, **Log Viewer**. Diese Datei wird über das Pull-Down-Menü **Bearbeiten => Einstellungen** in **Log Viewer** bearbeitet. Die Bearbeitung sollte nicht manuell erfolgen. Weitere Informationen zum Verwenden der Anwendung finden Sie im Kapitel *Protokolldateien* des *Red Hat Enterprise Linux Handbuch zur System-Administration*.

4.1.30. /etc/sysconfig/samba

Die Datei /etc/sysconfig/samba wird verwendet, um beim Booten Argumente an die Daemonen smbd und nmbd zu übertragen. Mit Hilfe des smbd-Daemonen können Windows-Clients im Netzwerk Verbindungen mit gemeinsamen Dateien herstellen. Mit dem nmbd-Daemonen steht Ihnen NetBIOS mit IP-Naming-Diensten zur Verfügung. Weitere Informationen zu den Parametern, die für diese Datei zur Verfügung stehen, erhalten Sie auf den man-Seiten von smbd. Standardmäßig sind smbd und nmbd so eingestellt, dass sie im Daemon-Modus ausgeführt werden.

4.1.31. /etc/sysconfig/sendmail

Die Datei /etc/sysconfig/sendmail ermöglicht das Versenden von Nachrichten an einen oder mehrere Empfänger, wobei die Nachrichten je nach Bedarf über beliebige Netzwerke geroutet werden können. In dieser Datei sind die Standardwerte für die Ausführung der Sendmail-Anwendung festgelegt. Standardmäßig läuft es als Hintergrund-Daemon und wird einmal stündlich überprüft, für den Fall, dass sich Nachrichten angesammelt haben.

Folgende Werte können verwendet werden:

- DAEMON=<*Wert*>, wobei <*Wert*> einer der folgenden booleschen Werte ist:
  - yes — Sendmail sollte so konfiguriert werden, dass er auf Port 25 eingehende Mails abfragt. Bei yes werden die -bd-Optionen von Sendmail verwendet.
  - no — Sendmail sollte nicht so konfiguriert werden, dass es auf Port 25 eingehende Mails abfragt.

- QUEUE=1h wird für Sendmail als -q$QUEUE eingestellt. Die -q-Option wird für Sendmail nicht eingestellt, wenn /etc/sysconfig/sendmail vorhanden ist und QUEUE leer oder nicht definiert ist.

4.1.32. /etc/sysconfig/spamassassin

Die Datei /etc/sysconfig/spamassassin wird verwendet, um Argumente zum spamd-Daemon (eine daemonisierte Version von Spamassassin) zur Bootzeit zu übergeben. Spamassassin ist ein Email-Spam-Filter. Eine Liste der verfügbaren Optionen finden Sie die auf den man-Seiten von spamd. Standardmäßig wird spamd für den Daemon-Mode konfiguriert, zum Erzeugen von Benuzter-Präferenzen und zum automatischen Erzeugen von Referenzlisten.

4.1.33. /etc/sysconfig/squid

Die Datei /etc/sysconfig/squid wird verwendet, um beim Booten Argumente an den squid-Daemon zu übertragen. Der squid-Daemon ist ein Proxy-Caching-Server für Web- Client-Applikationen. Weitere Informationen zum Konfigurieren eines squid-Proxy-Servers erhalten Sie, indem Sie mit einem Webbrowser das Verzeichnis /usr/share/doc/squid-<*Version*>/ öffnen (ersetzen Sie <*Version*> durch die auf Ihrem System installierte squid- Versionsnummer). Standardmäßig ist in dieser Datei der squid-Topstart im Daemon-Modus und die Zeitspanne, innerhalb der es sich schließt, festgelegt.

4.1.34. /etc/sysconfig/tux

/etc/sysconfig/tux ist die Konfigurationsdatei für den Red Hat Content Accelerator (früher TUX), den Kernel-basierten Web-Server. Weitere Informationen zum Konfigurieren von Red Hat Content Accelerator erhalten Sie, wenn Sie mit einem Web-Browser /usr/share/doc/tux-<*Version*>/tux/index.html öffnen (ersetzen Sie ><*Version*> mit der bereits auf Ihrem System installierten TUX-Versionsnummer). Die für diese Datei verfügbaren Parameter sind unter /usr/share/doc/tux-<*Version*>/tux/parameters.html aufgeführt.

4.1.35. /etc/sysconfig/vncservers

Die Datei /etc/sysconfig/vncservers konfiguriert, wie der *Virtual Network Computing* (*VNC*)-Server gestartet wird. Bei VNC handelt es sich um ein System zur Remote-Anzeige, mit der Sie eine Bildschirmumgebung nicht nur auf dem zugehörigen Rechner anzeigen können, sondern auch über

verschiedene Netzwerke (von LAN bis Internet) und dabei eine Vielfalt von Rechnerarchitekturen verwenden können.

VNC is a remote display system which allows users to view the desktop environment not only on the machine where it is running but across different networks on a variety of architectures.

Folgende Werte können enthalten sein:

- `VNCSERVERS=<Wert>`, wobei `<Wert>` z.B. wie folgt eingestellt wird: `"1:fred"`. Dies zeigt an, dass ein VNC-Server für den Benutzer Fred auf Anzeige :1 gestartet werden sollte. Benutzer Fred muss allerdings vorher mit `vncpasswd` ein VNC-Passwort eingestellt haben, um eine Verbindung mit dem Remote-VNC-Server herstellen zu können.

Beachten Sie bitte, dass Ihre Kommunikation nicht verschlüsselt ist, wenn Sie mit einem VNC-Server arbeiten. Sie sollten VNC also nicht auf einem unsicheren Netzwerk verwenden. Genaue Anweisungen hinsichtlich der Benutzung von SSH zum Schutz der Kommunikaton mit VNC finden Sie unter http://www.uk.research.att.com/vnc/sshvnc.html. Näheres über SSH finden Sie in Kapitel 17 oder im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

4.1.36. `/etc/sysconfig/xinetd`

Mit der Datei `/etc/sysconfig/xinetd` werden zum Zeitpunkt des Bootens Argumente an den `xinetd`-Daemon übertragen. Der `xinetd`-Daemon startet Programme, die Ihnen Internet-Dienste zur Verfügung stellen, wenn auf dem für diesen Dienst zuständigen Port eine entsprechende Anfrage eingeht. Weitere Informationen zu den verfügbaren Parametern dieser Datei erhalten Sie auf den man-Seiten von `xinetd`. Weitere Informationen zum `xinetd`-Dienst finden Sie unter Abschnitt 14.3.

4.2. Verzeichnisse im Verzeichnis `/etc/sysconfig/`

Folgende Verzeichnisse befinden sich normalerweise in `/etc/sysconfig/`:

- `apm-scripts/` — Dieses Verzeichnis enthält das Red Hat APM Suspend/Resume-Skript. Sie sollten diese Datei nicht direkt bearbeiten. Wenn Sie eine Anpassung wünschen, erstellen Sie eine Datei mit dem Namen `/etc/sysconfig/apm-scripts/apmcontinue`, die dann am Ende des Skripts aufgerufen wird. Sie können das Skript auch mittels der Bearbeitung von `/etc/sysconfig/apmd` steuern.
- `cbq/` — Dieses Verzeichnis enthält die Konfigurationsdateien für das Class Based Queuing im Rahmen der Verwaltung der Datenübertragungsrate von Netzwerk-Schnittstellen.
- `networking/` — Dieses Verzeichnis wird für **Network Administration Tool** (`redhat-config-network`)verwendet und sollte nicht manuell bearbeitet werden. Weitere Informationen zur Konfiguration von Schnittstellen mit **Network Administration Tool** finden Sie im Kapitel *Netzwerkkonfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.
- `network-scripts/` — Dieses Verzeichnis enthält die folgenden netzwerkrelevanten Konfigurationsdateien:
  - Netzwerk-Konfigurationsdateien für jede einzelne konfigurierte Schnittstelle, wie z.B. `ifcfg-eth0` für die `eth0`-Ethernet-Schnittstelle.
  - Skripts zur Aktivierung und Deaktivierung von Netzwerk-Schnittstellen, wie z.B. `ifup` und `ifdown`.
  - Skripts zur Aktivierung und Deaktivierung von ISDN-Schnittstellen, wie z.B. `ifup-isdn` und `ifdown-isdn`

- Verschiedene Skripte zu gemeinsam genutzten Netzwerk-Funktionen, die nicht unmittelbar berarbeitet werden sollten.

  Weitere Informationen zum Verzeichnis `network-scripts` finden Sie unter Kapitel 8.

- `rhn/` — Dieses Verzeichnis enthält die Konfigurationsdateien für Red Hat Network Keine der Dateien in diesem Verzeichnis sollte manuell bearbeitet werden. Weitere Informationen zum Red Hat Network finden Sie auf der Red Hat Network-Website unter folgender URL: https://rhn.redhat.com.

4.3. Zusätzliche Ressourcen

Dieses Kapitel soll nur eine Einleitung zu den Dateien im Verzeichnis `/etc/sysconfig/` darstellen. Die folgende Informationsquelle enthält ausführlichere Informationen.

4.3.1. Installierte Dokumentation

- `/usr/share/doc/initscripts-`<*version-number*>`/sysconfig.txt` — Diese Datei enthält eine umfangreichere Liste der im Verzeichnis `/etc/sysconfig/` enthaltenen Dateien und die Konfigurationsoptionen, welche diesen zur Verfügung stehen. <*version-number*> im Pfad zur Datei entspricht der Version des installierten `initscripts`-Pakets.

redhat

Kapitel 5.

Das `proc` Dateisystem

Der Linux-Kernel hat zwei Hauptfunktionen: die Zugriffskontrolle auf physische Geräte eines Computers und die Planung wann und wie Prozesse diese Geräte beeinflussen. Das Verzeichnis `/proc/` enthält eine Hierarchie spezieller Dateien, die den aktuellen Stand des Kernel darstellen und Anwendungen und Benutzern einen Einblick in die Sicht des Kernels auf das System gestatten.

Im Verzeichnis `/proc/` finden Sie eine Vielzahl an Informationen zur Systemhardware und allen derzeit laufenden Prozessen. Außerdem können einige Dateien des Baumverzeichnisses `/proc/` von Benutzern und Anwendungen so geändert werden, dass sich die Kernelkonfiguration ändert.

5.1. Ein virtuelles Dateisystem

Unter Linux werden alle Daten in Dateien gespeichert. Die meisten Benutzer kennen die beiden Grundarten von Dateien - Text und Binär. Das `/proc` Verzeichnis enthält allerdings eine andere Dateiart, die *Virtuelle Datei* genannt wird. Aus diesem Grund spricht man bei `/proc/` oft von einem *Virtuellen Dateisystem*.

Diese virtuellen Dateien haben einige interessante Besonderheiten. Die meisten werden mit einer Dateigröße von 0 Bytes aufgelistet, wenn man die Datei allerdings öffnet, zeigt sie oft einiges an Informationen. Außerdem spiegeln die meisten Zeit-und Datumseinstellungen der virtuellen Dateien die aktuelle Zeit und das aktuelle Datum wieder, was bedeutet, dass sie sich ständig ändern.

Virtuelle Dateien wie `/proc/interrupts`, `/proc/meminfo`, `/proc/mounts` und `/proc/partitions` bieten einen aktuellen Einblick in die Systemumgebung. Andere, wie `/proc/filesystems` und das Verzeichnis `/proc/sys/` bieten Informationen zur System-Konfiguration und zu Schnittstellen.

Um eine bessere Strukturierung zu erreichen, sind Dateien mit ähnlichen Informationen in virtuelle Verzeichnisse und Unter-Verzeichnisse einsortiert. Zum Beispiel `/proc/ide` enthält Informationen zu allen physischen IDE Geräten. Prozessverzeichnisse enthalten Informationen zu jedem im System laufenden Prozess.

5.1.1. Anzeigen virtueller Dateien

Mit `cat`, `more` oder `less` können Sie die Dateien in `/proc/` mit ihrem enormen Informationsgehalt über das System direkt auslesen. Wenn Sie z.B. wissen möchten, welche Art von CPU ein Computer hat, geben Sie den Befehl `cat /proc/cpuinfo` ein, und es erscheint in etwa Folgendes:

```
processor : 0
vendor_id : AuthenticAMD
cpu family : 5
model  : 9
model name : AMD-K6(tm) 3D+ Processor
stepping : 1
cpu MHz  : 400.919
cache size : 256 KB
fdiv_bug : no
hlt_bug  : no
f00f_bug : no
coma_bug : no
fpu  : yes
fpu_exception : yes
cpuid level : 1
```

```
wp  : yes
flags  : fpu vme de pse tsc msr mce cx8 pge mmx syscall 3dnow k6_mtrr
bogomips : 799.53
```

Bei der Anzeige unterschiedlicher virtueller Dateien im Dateisystem `/proc/` werden Sie feststellen, dass einige Informationen leicht verständlich sind, andere wiederum nicht lesbar sind. Aus diesem Grund gibt es Dienstprogramme, mit deren Hilfe Daten aus virtuellen Dateien lesbar angezeigt werden. Beispiele für diese Applikationen sind `lspci`, `apm`, `free` und `top`.

Anmerkung

Einige virtuelle Dateien im `/proc` können nur vom root gelesen werden.

5.1.2. Ändern virtueller Dateien

Im Allgemeinen sind die meisten virtuellen Dateien im Verzeichnis `/proc` schreibgschützt. Einige können jedoch dazu verwendet werden, Änderungen der Kernel-Einstellungen vorzunehmen. Das gilt im Besonderen für Dateien im Unterverzeichnis `/proc/sys/`.

Sie können den Wert einer virtuellen Datei ändern, indem Sie den neuen Wert mit dem Befehl `echo`, gefolgt von dem größer-als Symbol (>), an die gegebene Datei weiterleiten. Um zum Beispiel den Hostnamen zu ändern, geben Sie Folgendes ein:

```
echo www.example.com > /proc/sys/kernel/hostname
```

Andere Dateien funktionieren als binäre oder Boolesche Switches. Wenn Sie z.B. `cat /proc/sys/net/ipv4/ip_forward` eingeben, erscheint entweder `0` oder `1`. `0` gibt an, dass der Kernel keine Netzwerk-Pakete weiterleitet. Mit dem Befehl `echo` zum Ändern des Wertes der Datei `ip_forward` in `1` können Sie das Weiterleiten von Paketen sofort einschalten.

Tipp

Eine weiterer Befehl zur Änderung von Einstellungen im Unterverzeichnis `/proc/sys/` ist `/sbin/sysctl`. Weitere Informationen zu diesem Befehl erhalten Sie unter Abschnitt 5.4

Eine Liste einiger Kernel-Konfigurationsdateien, die in `/proc/sys/` enthalten sind, finden Sie unter Abschnitt 5.3.9.

5.2. Dateien im Hauptverzeichnis des proc Dateisystems

Im Folgenden finden Sie eine Liste von einigen nützlichen virtuellen Dateien im Top-Level des Verzeichnisses `/proc`.

Anmerkung

In den meisten Fällen entspricht der Inhalt der in diesem Abschnitt aufgeführten Dateien nicht denen in Ihrem Rechner. Dies liegt daran, dass sich die meisten Informationen auf die Hardware beziehen, auf der Red Hat Enterprise Linux läuft.

5.2.1. /proc/apm

Diese Datei bietet Informationen über den Status des *Advanced Power Management (APM)* Systems und wird vom Befehl `apm` benutzt. Die Ausgabe dieser Datei auf einem System ohne Akku, das an das Stromnetz angeschlossen ist, sieht ähnlich dieser Ausgabe aus:

```
1.16 1.2 0x07 0x01 0xff 0x80 -1% -1 ?
```

Wenn Sie den Befehl `apm -v` auf diesen Systemen ausführen, wird Folgendes angezeigt:

```
APM BIOS 1.2 (kernel driver 1.16)
AC on-line, no system battery
```

Auf nicht batteriebetriebenen Systemen kann `apm` nicht viel mehr bewirken, als den Rechner in den Standby-Modus zu versetzen. Der `apm` Befehl ist auf Laptops viel sinnvoller einzusetzen. Das zeigt auch die folgende Ausgabe von `cat /proc/apm`. Dies ist eine beispielhafte Ausgabe eines Laptops, der mit dem Stromnetz verbunden ist.

```
1.16 1.2 0x03 0x01 0x03 0x09 100% -1 ?
```

Wird das gleiche Laptop für einige Minuten vom Stromnetz entfernt, ändert sich der Inhalt der Datei `apm` wie folgt:

```
1.16 1.2 0x03 0x00 0x00 0x01 99% 1792 min
```

Der Befehl `apm -v` bietet eine informativere Ausgabe, wie Folgend:

```
APM BIOS 1.2 (kernel driver 1.16)
AC off-line, battery status high: 99% (1 day, 5:52)
```

5.2.2. /proc/cmdline

Diese Datei zeigt die Parameter an, die dem Linux-Kernel zum Startzeitpunkt übergeben wurden. Eine `/proc/cmdline` Beispieldatei sieht wie folgt aus:

```
ro root=/dev/hda2
```

`(ro)`; zeigt an, dass der Kernel read-only von der zweiten Partition auf dem ersten IDE Device `/dev/hda2` geladen wurde.

5.2.3. /proc/cpuinfo

Diese virtuelle Datei identifiziert den von Ihrem System verwendeten Prozessor. Eine typische Ausgabe sieht zum Beispiel wie folgt aus:

```
processor : 0
vendor_id : GenuineIntel
```

```
cpu family : 15
model  : 2
model name : Intel(R) Xeon(TM) CPU 2.40GHz
stepping : 7
cpu MHz  : 2392.371
cache size : 512 KB
physical id : 0
siblings : 2
runqueue : 0
fdiv_bug : no
hlt_bug  : no
f00f_bug : no
coma_bug : no
fpu  : yes
fpu_exception : yes
cpuid level : 2
wp  : yes
flags  : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm
bogomips : 4771.02
```

- `processor` — Gibt jedem Prozessor eine ID-Nummer. Wenn Ihr System nur über einen Prozessor verfügt, wird nur `0` angezeigt.
- `cpu family` — Zeigt Ihnen den Prozessortyp an, den Ihr System benutzt. Basiert Ihr Rechner auf Intel, stellen Sie die Zahl einfach vor "86", um den Wert zu berechnen. Das ist besonders dann nützlich, wenn Sie die Architektur eines älteren Systems, wie 586, 486, oder 386, herausfinden möchten. Da einige RPM Pakete für jede dieser speziellen Architekturen kompiliert werden, hilft Ihnen dieser Wert bei der Entscheidung, welches Packet zu installieren ist.
- `model name` — Zeigt den Namen und den Projektnamen des Prozessors an.
- `cpu MHz` — Zeigt die genaue Geschwindigkeit des Prozessors in Megahertz an.
- `cache size` — Zeigt die Menge von verfügbarem Level 2 Cache des Prozessors an.
- `siblings` — Zeigt die Anzahl von "sibling" CPUs auf der gleichen physischen CPU für Architekturen, die Hyper-Threading verwenden, an.
- `flags` — Gibt eine Anzahl von Eigenschaften des Prozessors aus, wie zum Beispiel eine Floating Point Unit (FPU), oder die Verarbeitung von MMX-Befehlen.

5.2.4. `/proc/devices`

Diese Datei zeigt die Zeichen- und Block-Geräte an, die zur Zeit im Kernel konfiguriert sind (Geräte, deren Module nicht im Kernel geladen sind, werden nicht berücksichtigt). Eine Beispiel-Ausgabe dieser virtuellen Datei finden Sie hier:

```
Character devices:
  1 mem
  2 pty
  3 ttyp
  4 ttyS
  5 cua
  7 vcs
 10 misc
 14 sound
 29 fb
```

```
 36 netlink
128 ptm
129 ptm
136 pts
137 pts
162 raw
254 iscsictl

Block devices:
  1 ramdisk
  2 fd
  3 ide0
  9 md
 22 ide1
```

Die Ausgabe von `/proc/devices` enthält die Major Number und den Namen eines Gerätes und ist in zwei größere Sektionen aufgeteilt: `Character devices` und `Block devices`.

Zeichen-Geräte (Character Devices) sind bis auf zwei wichtige Unterschiede sehr ähnlich zu *Block-Geräten*.

1. Block-Geräte haben einen Puffer, der das Ordnen von Zugriffen vor der Ausführung zulässt. Das ermöglicht zum Beispiel bei Festplatten oder anderen Speichergeräten eine effizientere Speicherung. Zeichen-Geräte benötigen diese Pufferung nicht.
2. Block-Geräte können Informationen in Datenblöcken einer bestimmten Größe senden und empfangen. Diese Größe kann je nach Gerät konfiguriert werden. Zeichen-Geräte senden Daten, ohne eine vorkonfigurierte Größe zu beachten.

Für weitere Informationen über Geräte, sehen Sie die im Folgenden angegebene Dokumentation:

```
/usr/src/linux-2.4/Documentation/devices.txt
```

5.2.5. `/proc/dma`

Diese Datei enthält eine Liste von registrierten ISA Direct Memory Access (DMA) Kanälen, die verwendet werden. Eine Beispieldatei von `/proc/dma` sieht wie folgt aus:

```
 4: cascade
```

5.2.6. `/proc/execdomains`

Diese Datei zeigt die *Execution Domains*, die gegenwärtig vom Linux-Kernel unterstützt werden, und die jeweilige Anzahl unterstützter "Personalities" (Persönlichkeiten) an.

```
0-0   Linux           [kernel]
```

Betrachten Sie Execution Domains als "Persönlichkeit" eines bestimmten Betriebssystems. Da andere Binär-Formate wie Solaris, UnixWare oder FreeBSD mit Linux verwendet werden können, kann ein Programmierer die Art verändern, wie das Betriebssystem bestimmte Systemaufrufe dieser Binärformate behandelt, in dem er die Persönlichkeit eines Tasks ändert. Bis auf die Execution Domain `PER_LINUX` können unterschiedliche Persönlichkeiten als dynamisch ladbare Module implementiert werden.

5.2.7. /proc/fb

Diese Datei enthält eine Liste von Framebuffer-Geräten, inklusive der Framebuffer-Gerätenummer und dem zuständigen Treiber. Eine typische Ausgabe von `/proc/fb` für ein System mit einem Framebuffer-Gerät sieht wie folgt oder ähnlich aus:

```
0 VESA VGA
```

5.2.8. /proc/filesystems

Diese Datei zeigt eine Liste von Dateisystemen an, die zur Zeit vom Kernel unterstützt werden. Eine Beispielausgabe mit einem generischen `/proc/filesystems` sieht ähnlich wie folgendes aus:

```
nodev rootfs
nodev bdev
nodev proc
nodev sockfs
nodev tmpfs
nodev shm
nodev pipefs
 ext2
nodev ramfs
 iso9660
nodev devpts
 ext3
nodev autofs
nodev binfmt_misc
```

Die erste Spalte zeigt an, ob die Dateisysteme auf einem Block-Gerät liegen; wenn in der ersten Spalte `nodev` steht, bedeutet das, dass Sie nicht auf ein Block-Gerät gemountet sind. Die zweite Spalte zeigt die Namen des unterstützten Dateisystems an.

Der `mount` Befehl durchsucht die hier aufgelisteten Dateisysteme, wenn keines als Argument angegeben wurde.

5.2.9. /proc/interrupts

Diese Datei zeigt die Anzahl von Interrupts pro IRQ auf der x86 Architektur an. Eine typische `/proc/interrupts` Datei ähnelt dem Folgenden:

```
           CPU0
  0:   80448940          XT-PIC  timer
  1:     174412          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          1          XT-PIC  rtc
 10:     410964          XT-PIC  eth0
 12:      60330          XT-PIC  PS/2 Mouse
 14:    1314121          XT-PIC  ide0
 15:    5195422          XT-PIC  ide1
NMI:          0
ERR:          0
```

Bei einer Multi-Prozessor-Maschine sieht dies etwas anders aus:

```
           CPU0       CPU1
  0: 1366814704          0          XT-PIC  timer
```

```
  1:        128        340   IO-APIC-edge  keyboard
  2:          0          0         XT-PIC  cascade
  8:          0          1   IO-APIC-edge  rtc
 12:       5323       5793   IO-APIC-edge  PS/2 Mouse
 13:          1          0         XT-PIC  fpu
 16:   11184294   15940594   IO-APIC-level  Intel EtherExpress Pro 10/100 Ethernet
 20:    8450043   11120093   IO-APIC-level  megaraid
 30:      10432      10722   IO-APIC-level  aic7xxx
 31:         23         22   IO-APIC-level  aic7xxx
NMI:          0
ERR:          0
```

Die erste Spalte bezeichnet die IRQ Nummer. Jeder CPU im Rechner hat seine eigene Spalte und seine eigenen Interrupts pro IRQ. Die nächste Spalte bezeichnet den Typ des Interrupts und die letzte Spalte enthält den Namen des Geräts, das auf diesem IRQ angesprochen werden kann.

Jeder der Interrupt-Typen, die plattform-spezifisch sind, in dieser Datei hat eine unterschiedliche Bedeutung. Bei x86 Rechnern kommen folgende Werte häufig vor:

- `XT-PIC` — Die alten AT-Rechner Interrupts.
- `IO-APIC-edge` — Das Spannungssignal dieses Interrupts variiert zwischen tief und hoch, und hat eine *Flanke*, an der der Interrupt ausgelöst und nur einmal signalisiert wird. Dieser Interrupt-Typ wird wie der `IO-APIC-level` Interrupt nur auf Systemen mit Prozessoren der 586 Familie und höher benutzt.
- `IO-APIC-level` — Erzeugt Interrupts, wenn das Spannungssignal hoch geht, solange, bis das Signal wieder niedrig ist.

5.2.10. `/proc/iomem`

Diese Datei zeigt Ihnen das aktuelle Mapping des Systemspeichers für jedes physische Gerät an:

```
00000000-0009fbff : System RAM
0009fc00-0009ffff : reserved
000a0000-000bffff : Video RAM area
000c0000-000c7fff : Video ROM
000f0000-000fffff : System ROM
00100000-07ffffff : System RAM
  00100000-00291ba8 : Kernel code
  00291ba9-002e09cb : Kernel data
e0000000-e3ffffff : VIA Technologies, Inc. VT82C597 [Apollo VP3]
e4000000-e7ffffff : PCI Bus #01
  e4000000-e4003fff : Matrox Graphics, Inc. MGA G200 AGP
  e5000000-e57fffff : Matrox Graphics, Inc. MGA G200 AGP
e8000000-e8ffffff : PCI Bus #01
  e8000000-e8ffffff : Matrox Graphics, Inc. MGA G200 AGP
ea000000-ea00007f : Digital Equipment Corporation DECchip 21140 [FasterNet]
  ea000000-ea00007f : tulip
ffff0000-ffffffff : reserved
```

Die erste Spalte zeigt die Speicherregister an, die von jedem der verschiedenen Speichertypen verwendet werden. Die zweite Spalte zeigt die Art des Speichers in diesem Register an. Diese Spalte zeigt Ihnen vor allem auch an, welche Speicherregister vom Kernel im Systemspeicher benutzt werden, oder, wenn z.B. Ihre Netzwerkschnittstelle mehrere Ethernetports hat, welcher Port welche Speicherregister verwendet.

5.2.11. /proc/ioports

Die Ausgabe von /proc/ioports liefert eine Liste von zur Zeit registrierten Port-Regionen zur I/O Kommunikation mit einem Gerät. Diese Datei kann sehr lang sein; der Anfang kann ähnlich wie hier aussehen:

```
0000-001f : dma1
0020-003f : pic1
0040-005f : timer
0060-006f : keyboard
0070-007f : rtc
0080-008f : dma page reg
00a0-00bf : pic2
00c0-00df : dma2
00f0-00ff : fpu
0170-0177 : ide1
01f0-01f7 : ide0
02f8-02ff : serial(auto)
0376-0376 : ide1
03c0-03df : vga+
03f6-03f6 : ide0
03f8-03ff : serial(auto)
0cf8-0cff : PCI conf1
d000-dfff : PCI Bus #01
e000-e00f : VIA Technologies, Inc. Bus Master IDE
  e000-e007 : ide0
  e008-e00f : ide1
e800-e87f : Digital Equipment Corporation DECchip 21140 [FasterNet]
  e800-e87f : tulip
```

Die erste Spalte zeigt den Adressbereich des I/O-Ports an, der für ein Gerät in der zweiten Spalte reserviert ist.

5.2.12. /proc/isapnp

Diese Datei listet *Plug and Play (PnP)* Karten in ISA Steckplätzen im System auf. Dies ist oft bei Soundkarten der Fall, aber kann auch viele andere Geräte umfassen. Eine /proc/isapnp Datei mit einem Soundblaster-Eintrag sieht ähnlich wie hier aus:

```
Card 1 'CTL0070:Creative ViBRA16C PnP' PnP version 1.0 Product version 1.0
  Logical device 0 'CTL0001:Audio'
    Device is not active
    Active port 0x220,0x330,0x388
    Active IRQ 5 [0x2]
    Active DMA 1,5
    Resources 0
      Priority preferred
      Port 0x220-0x220, align 0x0, size 0x10, 16-bit address decoding
      Port 0x330-0x330, align 0x0, size 0x2, 16-bit address decoding
      Port 0x388-0x3f8, align 0x0, size 0x4, 16-bit address decoding
      IRQ 5 High-Edge
      DMA 1 8-bit byte-count compatible
      DMA 5 16-bit word-count compatible
      Alternate resources 0:1
        Priority acceptable
        Port 0x220-0x280, align 0x1f, size 0x10, 16-bit address decoding
        Port 0x300-0x330, align 0x2f, size 0x2, 16-bit address decoding
```

```
Port 0x388-0x3f8, align 0x0, size 0x4, 16-bit address decoding
IRQ 5,7,2/9,10 High-Edge
DMA 1,3 8-bit byte-count compatible
DMA 5,7 16-bit word-count compatible
```

Diese Datei kann sehr lang werden, je nach Anzahl der angezeigten Geräte und deren Ressourcenanforderungen.

Jede Karte wird mit ihrem Namen, der PnP-Versionsnummer und der Produkt-Versionsnummer angezeigt. Wenn das Gerät aktiv und konfiguriert ist, zeigt die Datei auch den Port und die IRQs der Karte an. Zusätzlich zeigt die Karte auch `preferred` und `acceptable` Werte für verschiedene Parameter an. Das Ziel hierbei ist, PnP Karten perfekt einzustellen und Konflikte für IRQ und Ports zu vermeiden.

5.2.13. `/proc/kcore`

Diese Datei repräsentiert den physischen Speicher des Systems und wir im core-Dateiformat abgespeichert. Im Gegensatz zu den meisten `/proc` Dateien, zeigt `kcore` seine Größe an. Dieser Wert wird in Bytes angezeigt und entspricht der Größe des physischen Speichers (RAM) plus 4KB.

Der Inhalt dieser Datei ist so konzipiert, dass er nur von einem Debugger wie `gdb` untersucht werden kann, und ansonsten nicht lesbar ist.

Warnung

Öffnen Sie die virtuelle Datei `/proc/kcore` nicht. Die Inhalte der Datei werden als Textausgabe unlesbar auf dem Bildschirm angezeigt. Wenn Sie diese Datei unbeabsichtigt öffnen, drücken Sie [Strg]-[C], um den Prozess zu stoppen und kehren Sie mit `reset` zum Befehlszeilenprompt zurück.

5.2.14. `/proc/kmsg`

In dieser Datei befinden sich Mitteilungen, die vom Kernel erstellt wurden. Diese Mitteilungen werden dann von anderen Programmen, wie z.B. `/sbin/klogd` oder `/bin/dmesg`, hier abgerufen.

5.2.15. `/proc/ksyms`

Diese Datei enthält die vom Kernel exportierten Symbol-Definitionen, die von den Modul-Programmen benutzt werden, um ladbare Module dynamisch zu verlinken und einzubinden.

```
e003def4 speedo_debug [eepro100]
e003b04c eepro100_init [eepro100]
e00390c0 st_template [st]
e002104c RDINDOOR [megaraid]
e00210a4 callDone [megaraid]
e00226cc megaraid_detect [megaraid]
```

Der erste Spalte listet die Speicheradresse für die Kernelfunktion auf, die zweite Spalte bezieht sich auf den Namen der Funktion, und die letzte Spalte zeigt den Namen des geladenen Moduls an.

5.2.16. /proc/loadavg

Diese Datei bietet eine Übersicht über die durchschnittliche Auslastung der Prozessoren über Zeit, und liefert außerdem zusätzliche Informationen, die vom `uptime` und anderen Befehlen benutzt werden. Eine `/proc/loadavg`-Beispielsdatei finden Sie hier:

```
0.20 0.18 0.12 1/80 11206
```

Die ersten drei Spalten messen die CPU-Ausnutzung der letzten 1, 5 und 10 Minuten. Die vierte Spalte zeigt die Anzahl der zur Zeit laufenden Prozesse und die Gesamtanzahl der Prozesse an. Die letzte Spalte zeigt die letzte Prozess-ID, die verwendet wurde.

5.2.17. /proc/locks

Diese Datei zeigt die Dateien an, die zur Zeit vom Kernel gesperrt sind. Der Inhalt dieser Datei enthält interne Debugging-Daten des Kernels und kann stark variieren, je nach Benutzungsgrad des Systems. Eine Beispiel `/proc/locks` Datei eines Systems mit leichter Belastung finden Sie hier:

```
1: FLOCK  ADVISORY  WRITE 807 03:05:308731 0 EOF c2a260c0 c025aa48 c2a26120
2: POSIX  ADVISORY  WRITE 708 03:05:308720 0 EOF c2a2611c c2a260c4 c025aa48
```

Jeder Sperre wird eine einmalige Zahl am Anfang jeder Zeile zugeordnet. Die zweite Spalte zeigt den verwendeten Sperr-Typ an, wobei `FLOCK` für die älteren UNIX Dateisperren des `flock` Systemaufrufs steht. `POSIX` wiederum steht für die neueren POSIX-Sperren mit dem `lockf` Systemaufruf.

Die dritte Spalte kann zwei Werte haben: `ADVISORY` oder `MANDATORY`. `ADVISORY` bedeutet, dass die Sperre andere Benutzer nicht vom Datenzugriff abhält; nur andere Sperr-Versuche werden verhindert. `MANDATORY` bedeutet, dass kein anderer Datenzugriff zugelassen wird, solange die Sperre bestehen bleibt. Die vierte Spalte zeigt an, ob die Sperre dem Eigentümer Lese- oder Schreibzugriff (`READ` oder `WRITE`) erlaubt und die fünfte Spalte zeigt die ID des gesperrten Prozesses an. Die sechste Spalte zeigt die ID der gesperrten Datei, in folgendem Format an: *MAJOR-DEVICE*:*MINOR-DEVICE*:*INODE-NUMBER*. Die siebte Spalte zeigt Anfang und Ende der in der Datei gesperrten Region. Die übrigen Spalten zeigen auf Kernel-interne Datenstrukturen für spezielle Debugging-Funktionen und können ignoriert werden.

5.2.18. /proc/mdstat

Diese Datei enthält die aktuellen Informationen zu Konfigurationen mit mehreren Platten und RAID. Wenn Ihr System keine solche Konfiguration enthält, sieht Ihre `/proc/mdstat` Datei vermutlich so ähnlich aus:

```
Personalities :
read_ahead not set
unused devices: <none>
```

Diese Datei bleibt solange in dem o.g. Zustand bis Sie ein Software-RAID erstellt haben oder `md` existiert. Dann können Sie `/proc/mdstat` anzeigen, um sich ein Bild davon zu machen, was gerade mit Ihren `md`*X* RAID-Geräten passiert.

Die folgende `/proc/mdstat` Datei zeigt ein System mit dem Gerät `md0`, das als RAID 1 Gerät konfiguriert ist und zur Zeit die Platten neu synchronisiert:

```
Personalities : [linear] [raid1]
read_ahead 1024 sectors
md0: active raid1 sda2[1] sdb2[0] 9940 blocks [2/2] [UU] resync=1% finish=12.3min
algorithm 2 [3/3] [UUU]
```

```
unused devices: <none>
```

5.2.19. `/proc/meminfo`

Dies ist eine der eher häufig benutzten Dateien im Verzeichnis `/proc`, da sie viele wertvolle Informationen über die RAM-Auslastung des Systems ausgibt.

Die folgende virtuelle Datei `/proc/meminfo` stammt von einem System mit 256MB Ram und 384MB Swap-Space:

```
       total:     used:    free:   shared: buffers:  cached:
Mem:  128692224 121212928  7479296        0  9293824 47964160
Swap: 1103093760 32772096 1070321664
MemTotal:       125676 kB
MemFree:          7304 kB
MemShared:           0 kB
Buffers:          9076 kB
Cached:          34204 kB
SwapCached:      12636 kB
Active:          79352 kB
ActiveAnon:      57308 kB
ActiveCache:     22044 kB
Inact_dirty:       240 kB
Inact_laundry:   17468 kB
Inact_clean:       984 kB
Inact_target:    19608 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:       125676 kB
LowFree:          7304 kB
SwapTotal:     1077240 kB
SwapFree:      1045236 kB
HugePages_Total:     2
HugePages_Free:      2
Hugepagesize:     2096 kB
```

Viele der hier ausgegebenen Informationen werden von den Befehlen `free`, `top` und `ps` verwendet. Die Ausgabe von `free` ist sogar im Aufbau und Inhalt ähnlich wie `/proc/meminfo`. Wenn Sie die Datei `/proc/meminfo` direkt ansehen, können Sie noch mehr Details ansehen:

- `Mem` — Zeigt den aktuellen Status des physischen Arbeitsspeichers im System mit einer kompletten Auflistung vom gesamten, benutzem, gemeinsam genutzem, gepuffertem und Cache-Speicher in Bytes (total, used, free, shared, buffered und cached).
- `Swap` — Zeigt die gesamte, benutzte und freie Menge von Swap in Bytes an (total, used und free).
- `MemTotal` — Gesamte RAM-Größe in Kilobytes.
- `MemFree` — Die Menge von physischem RAM, die vom System nicht benutzt wird, in Kilobytes.
- `MemShared` — Wird ab Kernel 2.4 nicht mehr benutzt, aber aus Kompatibilitätsgründen immer noch angezeigt.
- `Buffers` — Die Größe der physischen RAM in Kilobytes, der für Dateipufferung verwendet wird.
- `Cached` — Die Menge der physischen RAM, die als Cache verwendet wird, in Kilobyte.
- `SwapCached` — Die Menge des als Cache verwendeten Swap, in Kilobyte.
- `Active` — Die Gesamtmenge des Puffer oder Page-Cache-Speicher in Kilobyte, der aktiv verwendet wird.

- Inact_dirty — Die Gesamtmenge von Puffer oder Cache-Seiten, die freigegeben werden können, in Kilobyte.
- Inact_laundry — Die Gesamtmenge von Puffer oder Cache Seiten, die in Kürze frei und verfügbar werden, in Kilobyte. Dies geschieht eventuell nachdem Platten-IO für diese Seiten beendet wurde.
- Inact_clean — Die Gesamtmenge von Puffer oder Cache Seiten, die definitiv frei und verfügbar sind, in Kilobyte.
- Inact_target — Netto-Menge von Zuordnungen pro Sekunden in Kilobyte, Durchschnitt pro Minute. Diese Statistik wurde überhohlt und hat auf modernen Systemen keine Bedeutung.
- HighTotal und HighFree — Die Gesamtmenge und der freie Speicher in Kilobytes, die nicht direkt in den Kernelbereich gemappt werden. Die Werte von HighTotal können von Kernel zu Kernel anders sein.
- LowTotal und LowFree — Die Gesamtmenge und der freie Speicher, die direkt in den Kernelbereich gemappt werden. Die Werte von LowTotal können von Kernel zu Kernel anders sein.
- SwapTotal — Die gesamte verfügbare Swapgröße, in Kilobyte.
- SwapFree — Die Gesamtmenge von freiem Swapspeicher, in Kilobyte.
- HugePages_Total — Die vollständige Anzahl von Hugepages für das System. Diese Nummer wird berechnet, indem Hugepagesize durch die Megabytes, die in /proc/sys/vm/hugetlb_pool für hugepages reserviert wurden, geteilt wird. Diese Statistik erscheint lediglich auf x86-, Itanium- und AMD64-Architekturen.
- HugePages_Free — Die vollständige Anzahl von Hugepages die dem System zur verfügung stehen. Diese Statistik erscheint lediglich auf x86-, Itanium- und AMD64-Architekturen.
- Hugepagesize — Die Größe für jede Hugepages-Einheit in Kilobytes. Der Standardwert ist 4096 KB auf Uniprocessor-Kernels für 32-Bit Architekturen. Für SMP und Hugemem-Kernel ist der Standardwert 2048 KB. Für 64-Bit Architekturen ist der Standardwert 262144 KB. Diese Statistik erscheint lediglich auf x86-, Itanium- und AMD64-Architekturen.

5.2.20. /proc/misc

Diese Datei listet verschiedene Treiber auf, die im Major-Gerät mit der Nummer 10 aufgeführt sind:

```
135 rtc
  1 psaux
134 apm_bios
```

Die erste Spalte zeigt die Minor-Nummer des Geräts an und die zweite Spalte zeigt den benutzten Treiber an.

5.2.21. /proc/modules

Diese Datei zeigt eine Liste aller Module an, die im Kernel geladen wurden. Ihr Inhalt hängt von der Konfiguration und vom System ab; die Organisation sollte aber ähnlich sein wie in dieser Ausgabe von /proc/modules:

```
ide-cd                 27008   0 (autoclean)
cdrom                  28960   0 (autoclean) [ide-cd]
soundcore               4100   0 (autoclean)
agpgart                31072   0 (unused)
binfmt_misc             5956   1
iscsi                  32672   0 (unused)
```

```
scsi_mod                94424   1 [iscsi]
autofs                  10628   0 (autoclean) (unused)
tulip                   48608   1
ext3                    60352   2
jbd                     39192   2 [ext3]
```

Die erste Spalte enthält den Namen des Moduls. Die zweite Spalte zeigt die Speichergröße des Moduls in Byte an. Die dritte Spalte zeigt an, ob das Modul zur Zeit geladen (`1`) oder nicht geladen (`0`) ist. Die letzte Spalte zeigt an, ob sich das Modul automatisch nach einer Zeit deaktivieren kann (`autoclean`) oder ob es zur Zeit nicht benutzt wird (`unused`). Jedes Modul mit einer Zeile, in der ein Name in Klammern (`[` und `]`) steht, zeigt an, dass dieses Modul ein anderes zum ordnungsgemäßen Funktionieren benötigt.

Diese Information kann auch mit dem Befehl `/sbin/lsmod` angezeigt werden.

5.2.22. `/proc/mounts`

Diese Datei gibt Ihnen einen kurzen Überblick über alle Mounts im System:

```
rootfs / rootfs rw 0 0
/dev/hda2 / ext3 rw 0 0
/proc /proc proc rw 0 0
/dev/hda1 /boot ext3 rw 0 0
none /dev/pts devpts rw 0 0
none /dev/shm tmpfs rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
```

Die Ausgabe aus dieser Datei ist sehr ähnlich zur Ausgabe von `/etc/mtab`, mit dem Unterschied, dass `/proc/mount` aktueller sein kann.

Die erste Spalte bezeichnet das Gerät das gemountet ist, wobei die zweite Spalte den zugehörigen Mount-Punkt anzeigt. Die dritte Spalte enthält den Dateisystemtyp und die vierte Spalte zeigt an, ob ein Dateisystem nur zum Lesen (`ro`) oder auch zum Schreiben (`rw`) gemountet ist. Die fünfte und sechste Spalte sind Dummy-Werte um das Format von `/etc/mtab` zu emulieren.

5.2.23. `/proc/mtrr`

Diese Datei bezieht sich auf die aktuellen Memory Type Range Registers (MTRRs), die im System verwendet werden. Wenn Ihre System Architektur MTRRs unterstüzt, könnte Ihre Datei `/proc/mtrr` so ähnlich wie diese aussehen:

```
reg00: base=0x00000000 (   0MB), size=  64MB: write-back, count=1
```

MTRRs werden seit der Intel P6 Familie benutzt (Pentium II und höher), um den Zugriff des Prozessors auf Speicherbereiche zu steuern. Wenn Sie eine Grafikkarte im PCI oder AGP Bus einsetzen, kann eine richtig konfigurierte `/proc/mtrr` Datei die Leistung um 150% erhöhen.

In den meisten Fällen werden diese Werte richtig für Sie eingestellt. Weitere Informationen zur manuellen Konfiguration dieser Datei, finden Sie unter folgender URL:

`http://web1.linuxhq.com/kernel/v2.3/doc/mtrr.txt.html`

5.2.24. /proc/partitions

Die meisten Infomationen hier sind nicht sehr wichtig für die meisten Benutzer. Die folgenden Zeilen allerdings ausgenommen:

- major — Die Major-Nummer des Gerätes, auf dem diese Partition liegt. Die Major-Nummer in unserem Beispiel (3) entspricht dem Block-Gerät ide0 in /proc/devices.
- minor — Die Minor-Nummer des Geräts, auf dem diese Partition liegt. Diese dient dazu, die Partionen auf verschiedene physische Geräte aufzuteilen und hängt mit der Zahl am Ende des Partitionsnamens zusammen.
- #blocks — Listet die Anzahl von Plattenblöcken auf, die in einer bestimmten Partition enthalten sind.
- name — Der Name der Partition.

5.2.25. /proc/pci

Diese Datei enthält eine volle Auflistung jedes PCI-Geräts in Ihrem System. Wenn Sie viele PCI-Geräte im System haben, kann /proc/pci sehr lang werden. Ein Beispiel aus dieser Datei auf einem Standardrechner:

```
Bus  0, device   0, function  0:
  Host bridge: Intel Corporation 440BX/ZX - 82443BX/ZX Host bridge (rev 3).
    Master Capable.  Latency=64.
    Prefetchable 32 bit memory at 0xe4000000 [0xe7ffffff].
Bus  0, device   1, function  0:
  PCI bridge: Intel Corporation 440BX/ZX - 82443BX/ZX AGP bridge (rev 3).
    Master Capable.  Latency=64.  Min Gnt=128.
Bus  0, device   4, function  0:
  ISA bridge: Intel Corporation 82371AB PIIX4 ISA (rev 2).
Bus  0, device   4, function  1:
  IDE interface: Intel Corporation 82371AB PIIX4 IDE (rev 1).
    Master Capable.  Latency=32.
    I/O at 0xd800 [0xd80f].
Bus  0, device   4, function  2:
  USB Controller: Intel Corporation 82371AB PIIX4 USB (rev 1).
    IRQ 5.
    Master Capable.  Latency=32.
    I/O at 0xd400 [0xd41f].
Bus  0, device   4, function  3:
  Bridge: Intel Corporation 82371AB PIIX4 ACPI (rev 2).
    IRQ 9.
Bus  0, device   9, function  0:
  Ethernet controller: Lite-On Communications Inc LNE100TX (rev 33).
    IRQ 5.
    Master Capable.  Latency=32.
    I/O at 0xd000 [0xd0ff].
    Non-prefetchable 32 bit memory at 0xe3000000 [0xe30000ff].
Bus  0, device  12, function  0:
  VGA compatible controller: S3 Inc. ViRGE/DX or /GX (rev 1).
    IRQ 11.
    Master Capable.  Latency=32.  Min Gnt=4.Max Lat=255.
    Non-prefetchable 32 bit memory at 0xdc000000 [0xdfffffff].
```

Diese Ausgabe zeigt eine Liste aller PCI-Geräte an, sortiert nach Bus, Gerät und Funktion. Außer Namen und Version eines Gerätes, gibt Ihnen diese Liste auch detaillierte IRQ-Informationen, so dass ein Administrator Konflikten schnell beikommen kann.

Tipp

Für eine besser lesbare Version dieser Informationen geben Sie Folgendes ein:

```
/sbin/lspci -vb
```

5.2.26. `/proc/slabinfo`

Diese Datei gibt Ihnen Informationen über die Speicherbenutzung im *slab* Level. Linux Kernel über 2.2 benutzen *slab pools*, um Speicher über der Page-Ebene zu verwalten. Oft benutzte Objekte haben dabei eigene Slab Pools. Es folgt ein Ausschnitt einer typischen virtuellen Datei `/proc/slabinfo`:

```
slabinfo - version: 1.1 (statistics)
kmem_cache            64      68    112    2    2    1
nfs_write_data         0       0    384    0    0    1
nfs_read_data          0     160    384    0   16    1
nfs_page               0     200     96    0    5    1
ip_fib_hash           10     113     32    1    1    1
journal_head          51    7020     48    2   90    1
revoke_table           2     253     12    1    1    1
revoke_record          0       0     32    0    0    1
clip_arp_cache         0       0    128    0    0    1
ip_mrt_cache           0       0     96    0    0    1
```

Die Werte in dieser Datei stehen in folgender Reihenfolge: Cache-Name, Anzahl der aktiven Objekte, Anzahl der Gesamtobjekte, Größe des Objekts, Anzahl der Aktiven slabs (Blöcke) des Objekts, Gesamtanzahl der slabs des Objekkts und Anzahl der Seiten per slab.

Beachten Sie bitte, dass *active* in diesem Fall bedeutet, dass ein Objekt "in Verwendung" ist.

5.2.27. `/proc/stat`

Diese Datei enthält diverse Statistiken über das System seit dem letzten Neustart. Der Inhalt von `/proc/stat`, welcher auch sehr lang sein kann, fängt ähnlich wie unser Beispiel an:

```
cpu  1139111 3689 234449 84378914
cpu0 1139111 3689 234449 84378914
page 2675248 8567956
swap 10022 19226
intr 93326523 85756163 174412 0 3 3 0 6 0 1 0 428620 0 60330 0 1368304 5538681
disk_io: (3,0):(1408049,445601,5349480,962448,17135856)
ctxt 27269477
btime 886490134
processes 206458
```

Einige der häufiger verwendeten Statistiken sind:

- `cpu` — Misst die Anzahl von *Jiffies* (1/100 Sekunden), in denen das System im Benutzer-Modus, Benutzer-Modus mit niedriger Priorität (nice), System Modus und im Idle-Task war. Die

Gesamtzahl für alle CPUs wird ganz oben ausgegeben und jede einzele CPU wird unten mit eigenen Statistiken aufgelistet.

- `page` — Anzahl der Speicherseiten, die das System von Platte und auf Platte geschrieben hat.
- `swap` — Anzahl der Swap-Seiten, die das System von Platte und auf Platte geschrieben hat.
- `intr` — Anzahl der Interrupts, die im System aufgetreten sind.
- `btime` — Die Boot-Zeit, gemessen in Sekunden seit dem 1 Januar 1970, auch bekannt als *epoch*.

5.2.28. /proc/sysrq-trigger

Unter Verwendung des Befehls `echo`, kann ein Remote-Benutzer System-Request-Key-Befehle wie an einem lokalen Terminal ausführen. Um mit `echo` den Wert in diese Datei zu schreiben, muss `/proc/sys/kernel/sysrq` auf einen Wert ungleich `0` gesetzt sein. Für weitere Informationen über den System-Request-Key, Sehen Sie Abschnitt 5.3.9.3.

Obwohl man zu dieser Datei schreiben kann, diese kann nicht gelesen werden, nicht einmal vom root-Benutzer.

5.2.29. /proc/swaps

Diese Datei misst den Swapspeicher und seine Auslastung. Für ein System mit nur einer Swap-Partition könnte die Ausgabe von `/proc/swap` ähnlich wie Folgt aussehen:

```
Filename     Type       Size    Used   Priority
/dev/hda6    partition  136512  20024  -1
```

Obwohl Sie einige dieser Informationen auch in anderen Dateien im Verzeichnis `/proc/` finden, liefert Ihnen die Datei `/proc/swap` einen Überblick über alle Swap-Dateinamen, Typen des Swap-Space und die Gesamtgröße sowie die verwendete Größe (in Kilobyte). Die Prioritätsspalte ist sinnvoll wenn mehrere Swap-Dateien benutzt werden. Je niedriger die Priorität, desto wahrscheinlicher wird eine Swap-Datei benutzt.

5.2.30. /proc/uptime

Diese Datei enthält Informationen darüber, wie lange das System seit dem letzten Neustart läuft. Die Ausgabe von `/proc/uptime` ist relativ gering:

```
350735.47 234388.90
```

Die erste Zahl zeigt die Sekundenzahl an, die das System bereits läuft. Die zweite Zahl zeigt die Sekunden an, wielange die Maschine idle (im Leerlauf) war.

5.2.31. /proc/version

Diese Datei zeigt die Version des Linux-Kernels und von `gcc` an und außerdem die Version von Red Hat Enterprise Linux, die auf dem System installiert ist:

```
Linux version 2.4.20-1.1931.2.231.2.12.ent (user@foo.redhat.com) (gcc version 3.2.3 200
(Red Hat Enterprise Linux 3.2.3-7)) #1 Thu Jun 19 14:57:04 EDT 2003
```

Diese Information wird für eine Vielzahl von Zwecken benutzt, unter anderem um Versionsdaten am Login-Prompt auszugeben.

5.3. Verzeichnisse in /proc/

Allgemeine Informationsgruppen bezüglich des Kernels werden in Verzeichnisse und Unterverzeichnisse in /proc sortiert.

5.3.1. Prozess-Verzeichnisse

Jedes /proc/ Verzeichnis enthält einige Verzeichnisse mit numerischen Namen. Eine Liste mit solchen fängt ähnlich dieser Liste an:

```
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 1
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 1010
dr-xr-xr-x    3 xfs      xfs             0 Feb 13 01:28 1087
dr-xr-xr-x    3 daemon   daemon          0 Feb 13 01:28 1123
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 11307
dr-xr-xr-x    3 apache   apache          0 Feb 13 01:28 13660
dr-xr-xr-x    3 rpc      rpc             0 Feb 13 01:28 637
dr-xr-xr-x    3 rpcuser  rpcuser         0 Feb 13 01:28 666
```

Diese Verzeichnisse heißen *Prozess-Verzeichnisse*, weil sie sich auf eine Prozess-ID beziehen und Informationen zu diesem Prozess enthalten. Der Eigentümer und die Gruppe jedes Prozess-Verzeichnisses wird auf die ID des Benutzers, der den Prozess ausführt, gesetzt. Wenn der Prozess beendet wird, verschwindet das zugehörige /proc Prozess-Verzeichnis.

Jedes Prozess-Verzeichnis enthält die folgenden Dateien:

- cmdline — Diese Datei enthält den Befehl, der bei Prozessstart ausgegeben wird.
- cpu — Bietet spezifische Informationen zur Prozessorlast aller CPUs an. Ein Prozess, der auf einem Dual-CPU-System läuft, könnte eine Ausgabe wie folgt haben:
  ```
  cpu  11 3
  cpu0 0 0
  cpu1 11 3
  ```
- cwd — Ein symbolischer Link zum aktuellen Arbeitsverzeichnis des Prozesses.
- environ — Gibt eine Liste von Umgebungsvariablen des Prozesses aus. Die Variablennamen werde in Großbuchstaben, die Werte in Kleinbuchstaben ausgegeben.
- exe — Ein symbolischer Link zur ausgeführten Datei des Prozesses.
- fd — Ein Verzeichnis mit allen Datei-Descriptors eines bestimmten Prozesses. Diese werden als nummerierte Links ausgegeben:
  ```
  total 0
  lrwx------    1 root     root           64 May  8 11:31 0 -> /dev/null
  lrwx------    1 root     root           64 May  8 11:31 1 -> /dev/null
  lrwx------    1 root     root           64 May  8 11:31 2 -> /dev/null
  lrwx------    1 root     root           64 May  8 11:31 3 -> /dev/ptmx
  lrwx------    1 root     root           64 May  8 11:31 4 -> socket:[7774817]
  lrwx------    1 root     root           64 May  8 11:31 5 -> /dev/ptmx
  lrwx------    1 root     root           64 May  8 11:31 6 -> socket:[7774829]
  lrwx------    1 root     root           64 May  8 11:31 7 -> /dev/ptmx
  ```
- maps — Enthält Speicher-Maps zu den verschiedenen ausführbaren Dateien und Library-Dateien, die mit diesem Prozess zusammenhängen. Diese Datei kann sehr lang werden, wenn ein sehr komplexer Prozess ausgeführt wird, eine Beispielausgabe eines sshd Prozesses fängt so an:
  ```
  08048000-08086000 r-xp 00000000 03:03 391479     /usr/sbin/sshd
  08086000-08088000 rw-p 0003e000 03:03 391479     /usr/sbin/sshd
  08088000-08095000 rwxp 00000000 00:00 0
  40000000-40013000 r-xp 00000000 03:03 293205     /lib/ld-2.2.5.so
  40013000-40014000 rw-p 00013000 03:03 293205     /lib/ld-2.2.5.so
  ```

```
40031000-40038000 r-xp 00000000 03:03 293282     /lib/libpam.so.0.75
40038000-40039000 rw-p 00006000 03:03 293282     /lib/libpam.so.0.75
40039000-4003a000 rw-p 00000000 00:00 0
4003a000-4003c000 r-xp 00000000 03:03 293218     /lib/libdl-2.2.5.so
4003c000-4003d000 rw-p 00001000 03:03 293218     /lib/libdl-2.2.5.so
```

- `mem` — Der Speicher, der von diesem Prozess benutzt wird. Diese Datei kann vom Benutzer nicht gelesen werden.
- `root` — Ein Link zum root Verzeichnis des Prozesses.
- `stat` — Der Status des Prozesses.
- `statm` — Der Status des Speichers, der von diesem Prozess benutzt wird. Eine beispielhafte `statm` Datei sieht aus wie folgt:
  ```
  263 210 210 5 0 205 0
  ```
  Die sieben Spalten hängen mit verschiedenen Speicherstatistiken für den Prozess zusammen. Sie zeigen von links nach rechts verschiedene Aspekte des benutzten Speichers:
  1. Gesamte Programmgröße, in Kilobytes.
  2. Größe der Speicherteile, in Kilobytes.
  3. Anzahl der gemeinsam verwendeten Seiten.
  4. Anzahl der Seiten mit Programmcode.
  5. Anzahl der Seiten mit Stack/Daten.
  6. Anzahl der Library-Seiten.
  7. Anzahl der unsauberen Seiten.

- `status` — Bietet den Status des Prozesses in einer lesbareren Form als `stat` oder `statm` an. Eine Beispielausgabe bei `sshd` sieht ähnlich wie folgt aus:
  ```
  Name: sshd
  State: S (sleeping)
  Tgid: 797
  Pid: 797
  PPid: 1
  TracerPid: 0
  Uid: 0 0 0 0
  Gid: 0 0 0 0
  FDSize: 32
  Groups:
  VmSize:     3072 kB
  VmLck:         0 kB
  VmRSS:      840 kB
  VmData:      104 kB
  VmStk:        12 kB
  VmExe:       300 kB
  VmLib:      2528 kB
  SigPnd: 0000000000000000
  SigBlk: 0000000000000000
  SigIgn: 8000000000001000
  SigCgt: 0000000000014005
  CapInh: 0000000000000000
  CapPrm: 00000000fffffeff
  CapEff: 00000000fffffeff
  ```
  Die Informationen in dieser Ausgabe enthalten den Prozessnamen, die ID, den Status (wie z.B. `S (sleeping)` oder `R (running)`, Benutzer/Gruppe die den Prozess ausführen, und detailierte Daten bezüglich der Speicherauslastung.

5.3.1.1. /proc/self/

Das Verzeichnis /proc/self ist ein Link zum zur Zeit laufenden Prozess. Das erlaubt einem Prozess, sich selbst zu beobachten, ohne die eigene Prozess-ID zu kennen.

In einer Shell-Umgebung hat eine Auflistung des Verzeichnises /proc/self den gleichen Inhalt wie die Auflistung des Prozess-Verzeichnisses dieses Prozesses.

5.3.2. /proc/bus/

Dieses Verzeichnis enthält spezifische Informationen zu den verschiedenen Bussystemen, die auf einem System verfügbar sind. Zum Beispiel finden Sie auf einem Standard-PC mit PCI- und USB-Bussen, aktuelle Daten zu jedem dieser Bussysteme in einem Unterverzeichnis von /proc/bus, das den Namen des Busses hat, wie z.B. /proc/bus/pci/.

Die Unterverzeichnisse und Dateien im Verzeichnis /proc/bus/ hängen von den zum System verbundenen Geräten ab. Jeder Bustyp hat jedoch zumindest ein Verzeichnis. Innerhalb dieser Bus-Verzeichnisse befindet sich zumindest ein Unterverzeichnis mit einem numerischen Namen, wie 001, das Binärdateien enthält.

Das Verzeichnis /proc/bus/usb/ enthält Dateien, die zu Geräten an den USB-Bussen gehören, genauso wie die Treiber, die gebraucht werden, um die Geräte zu benutzen. Folgend ist ein Beispiel eines /proc/bus/usb/-Verzeichnisses:

```
total 0
dr-xr-xr-x    1 root     root            0 May  3 16:25 001
-r--r--r--    1 root     root            0 May  3 16:25 devices
-r--r--r--    1 root     root            0 May  3 16:25 drivers
```

Das Verzeichnis /proc/bus/usb/001 enthält alle Geräte am ersten USB-Bus. Wenn Sie sich den Inhalt der Datei devices ansehen, können Sie sehen, dass es sich um das USB root Hub auf dem Mainboard handelt:

Folgend ist ein Beispiel der Datei /proc/bus/usb/devices:

```
T:  Bus=01 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#=  1 Spd=12  MxCh= 2
B:  Alloc=  0/900 us ( 0%), #Int=  0, #Iso=  0
D:  Ver= 1.00 Cls=09(hub  ) Sub=00 Prot=00 MxPS= 8 #Cfgs=  1
P:  Vendor=0000 ProdID=0000 Rev= 0.00
S:  Product=USB UHCI Root Hub
S:  SerialNumber=d400
C:* #Ifs= 1 Cfg#= 1 Atr=40 MxPwr=  0mA
I:  If#= 0 Alt= 0 #EPs= 1 Cls=09(hub  ) Sub=00 Prot=00 Driver=hub
E:  Ad=81(I) Atr=03(Int.) MxPS=   8 Ivl=255ms
```

5.3.3. /proc/driver/

Dieses Verzeichnis enthält Informationen zu bestimmten Treibern, die vom Kernel verwendet werden.

Eine allgemein hier zu findende Datei ist rtc, welche die Ausgabe des Treibers für die *Echtzeituhr (RTC)*, ein Gerät zum Erhalten der Zeit während der Rechner ausgeschaltet ist, darstellt. Eine Beispielausgabe von /proc/driver/rtc:

```
rtc_time : 01:38:43
rtc_date : 1998-02-13
rtc_epoch : 1900
alarm  : 00:00:00
```

```
DST_enable : no
BCD  : yes
24hr  : yes
square_wave : no
alarm_IRQ : no
update_IRQ : no
periodic_IRQ : no
periodic_freq : 1024
batt_status : okay
```

Informationen über den RTC finden Sie unter `/usr/src/linux-2.4/Documentation/rtc.txt`.

5.3.4. /proc/fs

Dieses Verzeichnis zeigt an, welche Dateisysteme exportiert werden. Arbeiten Sie mit einem NFS Server, geben Sie `cat /proc/fs/nfs/exports` ein, um die gemeinsam verwendeten Dateisysteme und die dafür gewährten Berechtigungen anzuzeigen. Weitere Informationen zur gemeinsamen Verwendung von Dateisystemen mit NFS finden Sie unter Kapitel 9.

5.3.5. /proc/ide/

Dieses Verzeichnis beinhaltet Informationen über IDE-Geräte auf diesem System. Jeder IDE-Kanal wird von einem seperaten Verzeichnis wie z.B. `/proc/ide/ide0` und `/proc/ide/ide1` repräsentiert. Zusätzlich gibt es eine `drivers` Datei, die die Versionsnummer der verschiedenen in diesem IDE-Kanal verwendeten Treiber darstellt:

```
ide-cdrom version 4.59
ide-floppy version 0.97
ide-disk version 1.10
```

Viele Chipsätze bieten eine Informationsdatei in diesem Verzeichnis an, welche zusätzliche Daten betreffend der Festplatten, die über die Kanäle angebunden sind, ausgibt. Zum Beispiel gibt ein generischer Intel PIIX4 Ultra 33 Chipsatz eine Datei `/proc/ide/piix` aus, die Ihnen zeigt, ob DMA oder UDMA für Geräte an den IDE-Kanälen aktiviert sind:

```
                                Intel PIIX4 Ultra 33 Chipset.
------------- Primary Channel ---------------- Secondary Channel -------------

                 enabled                           enabled
------------- drive0 --------- drive1 -------- drive0 ---------- drive1 ------

DMA enabled:    yes              no              yes               no
UDMA enabled:   yes              no              no                no
UDMA enabled:   2                X               X                 X
UDMA
DMA
PIO
```

Im Verzeichnis eines IDE-Kanals, wie z.B. `ide0` für den ersten Kanal, finden Sie noch mehr Informationen. Die Datei `channel` zeigt die Kanalnummer an, wohingegen die Datei `model` den Bustyp am Kanal anzeigt (z.B. `pci`).

5.3.5.1. Geräte-Verzeichnisse

In jedem IDE-Kanal-Verzeichnis befindet sich ein Geräte-Verzeichnis. Der Name des Geräte-Verzeichnisses entspricht dem Laufwerksbuchstaben im `/dev`-Verzeichnis. So ist z.B. das erste IDE-Laufwerk in `ide0 hda`.

Anmerkung

Für jedes dieser Geräte-Verzeichnisse gibt es einen symbolischen Link zum `/proc/ide/` Verzeichnis.

Jedes Geräte-Verzeichnis enthält eine Sammlung von Informationen und Statistiken. Der Inhalt dieser Verzeichnisse verändert sich je nach angesprochenem Gerät. Einige der wichtigen Dateien, die bei verschiedenen Geräten vorhanden sind, umfassen unter anderem:

- `cache` — Der Geräte-Cache.
- `capacity` — Die Kapazität des Gerätes in 512 Byte Blöcken.
- `driver` — Treiber und Treiberversion, die benutzt wird, um das Gerät anzusprechen.
- `geometry` — Physische und logische Geometrie des Gerätes.
- `media` — Der Geräte-Typ, wie zum Beispiel `disk`
- `model` — Modellname oder Nummer des Gerätes
- `settings` — Eine Liste von aktuellen Parametern des Gerätes. Diese Datei enthält normalerweise einige wissenswerte, technische Informationen. Ein Beispiel einer `settings` Datei für eine Standard IDE-Festplatte sieht so aus:

```
name                 value           min          max          mode
----                 -----           ---          ---          ----
bios_cyl             784             0            65535        rw
bios_head            255             0            255          rw
bios_sect            63              0            63           rw
breada_readahead     4               0            127          rw
bswap                0               0            1            r
current_speed        66              0            69           rw
file_readahead       0               0            2097151      rw
ide_scsi             0               0            1            rw
init_speed           66              0            69           rw
io_32bit             0               0            3            rw
keepsettings         0               0            1            rw
lun                  0               0            7            rw
max_kb_per_request   64              1            127          rw
multcount            8               0            8            rw
nice1                1               0            1            rw
nowerr               0               0            1            rw
number               0               0            3            rw
pio_mode             write-only      0            255          w
slow                 0               0            1            rw
unmaskirq            0               0            1            rw
using_dma            1               0            1            rw
```

5.3.6. /proc/irq/

Dieses Verzeichnis wird benutzt, um IRQ zu CPU Verbindungen einzustellen. Dies erlaubt Ihnen, einen IRQ nur einer CPU zuzuweisen. Sie können eine CPU aber z.B. auch vom IRQ-Handling entbinden.

Jeder IRQ hat ein eigenes Verzeichnis, was die individuelle Konfiguration jedes IRQ ermöglicht. Die Datei `/proc/irq/prof_cpu_mask` ist eine Bitmaske, die die Standardwerte für die Datei `smp_affinity` im IRQ-Verzeichnis enthält. Die Werte in `smp_affinity` legen fest, welche CPUs diesen IRQ bearbeiten.

Für weitere Informationen zum Verzeichnis `/proc/irq/`, sehen Sie:

```
/usr/src/linux-2.4/Documentation/filesystems/proc.txt
```

5.3.7. /proc/net/

Dieses Verzeichnis bietet einen weitgehenden Einblick in verschiedene Netzwerk-Parameter und -Statistiken. Jede Datei deckt einen bestimmten Informationsbereich zum Systemnetzwerkbereich ab. Es folgt eine Teilliste des Verzeichnisses `/proc/net/`:

- `arp` — Enthält die ARP-Tabelle des Kernels. Diese Datei ist besonders sinnvoll, um eine Hardware-Adresse einer IP-Adresse zuzuordnen.
- `atm` — Ein Verzeichnis, das Dateien mit verschiedenen Einstellungen und Statistiken zum *Asynchronous Transfer Mode (ATM)* enthält. Dieses Verzeichnis wird vor allem mit ATM-Netzkarten und ADSL-Karten benutzt.
- `dev` — Listet die verschiedenen Netzwerk-Geräte, die im System konfiguriert sind, mit Statistiken zum Senden und Empfangen, auf. Diese Datei zeigt Ihnen, welche Schnittstelle wieviel Bytes empfangen und gesendet hat, die Paketanzahl, Fehleranzahl und verlorene Pakete an.
- `dev_mcast` — Zeigt die verschiedenen Layer2 Multicast Gruppen an, auf denen ein Gerät zuhört.
- `igmp` — Listet die von diesem System zusammengefassten IP-Adressen auf.
- `ip_conntrack` — Listet gefundene Netzwerkverbindungen für Rechner mit weiterleitenden IP-Verbindungen auf.
- `ip_tables_names` — Listet die verwendeten Typen von `iptables`. Diese Datei besteht nur dann, wenn`iptables` auf dem System aktiv ist, und einen oder mehrere der folgenden Werte enthält: `filter`, `mangle`, oder `nat`.
- `ip_mr_cache` — Liste des Multicasting Routing Cache.
- `ip_mr_vif` — Liste der virtuellen Schnittstellen zum Multicasting.
- `netstat` — Enthält eine umfangreiche und detaillierte Sammlung von Netzwerk-Statistiken, mit TCP Timeouts, gesendeten und empfangenen SYN-Cookies und vielem mehr.
- `psched` — Liste der globalen Paket Scheduler Parametern.
- `raw` — Liste der Raw-Gerät Statistiken.
- `route` — Zeigt die Kernel-Routing-Tabelle an.
- `rt_cache` — Zeigt den aktuellen Routing Cache.
- `snmp` — Eine Liste von Simple Network Management Protocol (SNMP) Daten verschiedener Netzwerk-Protokolle.
- `sockstat` — Liefert Statistiken zum Socket.
- `tcp` — Enthält detaillierte Informationen zum TCP-Socket.

- `tr_rif` — Die Token Ring RIF Routing Tabelle.
- `udp` — Enthält detaillierte Informationen zum UDP-Socket.
- `unix` — Listet die UNIX-Domain-Sockets auf, die zur Zeit benutzt werden.
- `wireless` — Zeigt Informationen zu Wireless Interfaces.

5.3.8. `/proc/scsi/`

Dieses Verzeichnis ist analog zum Verzeichnis `/proc/ide/`, kann aber nur für verbundene SCSI-Geräte verwendet werden.

Die wichtigste Datei hier ist `/proc/scsi/scsi`, welche eine Liste mit allen erkannten SCSI-Geräten enthält. Aus dieser Auflistung können Sie den Typ des Gerätes, den Modell-Namen, den Hersteller und die SCSI Kanal/ID-Daten abrufen.

Wenn ein System zum Beispiel ein SCSI CD-ROM, ein Bandlaufwerk, Festplatten und einen RAID-Controller beinhaltet, könnte die Datei ähnlich wie in diesem Beispiel aussehen:

```
Attached devices:
Host: scsi1 Channel: 00 Id: 05 Lun: 00
  Vendor: NEC      Model: CD-ROM DRIVE:466 Rev: 1.06
  Type:   CD-ROM                           ANSI SCSI revision: 02
Host: scsi1 Channel: 00 Id: 06 Lun: 00
  Vendor: ARCHIVE  Model: Python 04106-XXX Rev: 7350
  Type:   Sequential-Access                ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 06 Lun: 00
  Vendor: DELL     Model: 1x6 U2W SCSI BP  Rev: 5.35
  Type:   Processor                        ANSI SCSI revision: 02
Host: scsi2 Channel: 02 Id: 00 Lun: 00
  Vendor: MegaRAID Model: LD0 RAID5 34556R Rev: 1.01
  Type:   Direct-Access                    ANSI SCSI revision: 02
```

Jeder SCSI-Treiber, der vom System benutzt wird, hat ein eigenes Verzeichnis in `/proc/scsi/`, welches spezifische Dateien für jeden Controller enthält. Für unser Beispiel oben gibt es also die Verzeichnisse `aic7xxx` und `megaraid`, da diese beiden Treiber benutzt werden. Die Dateien in diesen beiden Unterverzeichnissen beinhalten typischerweise I/O Adressbereiche, IRQ-Informationen und Statistiken für den SCSI-Controller, der den Treiber benutzt. Jeder Controller liefert Informationen in verschiedener Größe und Art. Der Adaptec AIC-7880 Ultra SCSI Hostadapter in unserem Beispiel gibt folgende Ausgabe:

```
Adaptec AIC7xxx driver version: 5.1.20/3.2.4
Compile Options:
  TCQ Enabled By Default : Disabled
  AIC7XXX_PROC_STATS     : Enabled
  AIC7XXX_RESET_DELAY    : 5

Adapter Configuration:
           SCSI Adapter: Adaptec AIC-7880 Ultra SCSI host adapter
                         Ultra Narrow Controller
    PCI MMAPed I/O Base: 0xfcffe000
 Adapter SEEPROM Config: SEEPROM found and used.
      Adaptec SCSI BIOS: Enabled
                    IRQ: 30
                   SCBs: Active 0, Max Active 1,
                         Allocated 15, HW 16, Page 255
             Interrupts: 33726
      BIOS Control Word: 0x18a6
```

```
   Adapter Control Word: 0x1c5f
   Extended Translation: Enabled
Disconnect Enable Flags: 0x00ff
     Ultra Enable Flags: 0x0020
 Tag Queue Enable Flags: 0x0000
Ordered Queue Tag Flags: 0x0000
Default Tag Queue Depth: 8
    Tagged Queue By Device array for aic7xxx host instance 1:
      {255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,255}
    Actual queue depth per device for aic7xxx host instance 1:
      {1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1}

Statistics:


(scsi1:0:5:0)
  Device using Narrow/Sync transfers at 20.0 MByte/sec, offset 15
  Transinfo settings: current(12/15/0/0), goal(12/15/0/0), user(12/15/0/0)
  Total transfers 0 (0 reads and 0 writes)
             < 2K      2K+     4K+     8K+    16K+    32K+    64K+   128K+
   Reads:       0        0       0       0       0       0       0       0
  Writes:       0        0       0       0       0       0       0       0


(scsi1:0:6:0)
  Device using Narrow/Sync transfers at 10.0 MByte/sec, offset 15
  Transinfo settings: current(25/15/0/0), goal(12/15/0/0), user(12/15/0/0)
  Total transfers 132 (0 reads and 132 writes)
             < 2K      2K+     4K+     8K+    16K+    32K+    64K+   128K+
   Reads:       0        0       0       0       0       0       0       0
  Writes:       0        0       0       1     131       0       0       0
```

Dieser Bildschirm zeigt die Transfergeschwindigkeiten zu den verschiedenen SCSI-Geräten, die an den Controller angeschlossen sind, basierend auf der Channel-ID, sowie detaillierte Statistiken zu der Anzahl und Größe der Dateien, die von diesem Gerät gelesen oder geschrieben wurden. Der oben angegebenen Ausgabe entnehmen Sie, dass der Controller mit dem CD-ROM-Laufwerk mit 20 Megabyte pro Sekunde kommuniziert, während das Bandlaufwerk nur mit 10 Megabytes kommuniziert.

5.3.9. /proc/sys/

Das Verzeichnis `/proc/sys/` unterscheidet sich von `/proc`, weil es nicht nur eine Menge Informationen über das System zeigt, sondern auch Administratoren erlaubt, Kerneleigenschaften sofort zu aktivieren oder zu deaktivieren.

Warnung

Versuchen Sie niemals, Ihre Kernel-Einstellungen auf einem Produktionssystem mit den Dateien in `/proc/sys` zu optimieren. Es kann in manchen Fällen passieren, dass eine Einstellung den Kernel instabil macht und damit ein Neustart erforderlich wird.

Überprüfen Sie daher unbedingt die Korrektheit der Syntax, bevor Sie eine Änderung in `/proc/sys` vornehmen.

Ob eine Datei konfiguriert werden kann oder nur Informationen liefern soll, findet man am besten heraus, indem man sie über `-l` an einem Shell-Prompt anzeigt. Wenn die Datei schreibbar ist, können Sie diese zum Konfigurieren des Kernels verwenden. Zum Beispiel sieht eine Auflistung von `/proc/sys/fs` so aus:

```
-r--r--r--    1 root     root            0 May 10 16:14 dentry-state
-rw-r--r--    1 root     root            0 May 10 16:14 dir-notify-enable
-r--r--r--    1 root     root            0 May 10 16:14 dquot-nr
-rw-r--r--    1 root     root            0 May 10 16:14 file-max
-r--r--r--    1 root     root            0 May 10 16:14 file-nr
```

Hier sind die Dateien `dir-notify-enable` und `file-max` schreibbar und können deshalb benutzt werden, um den Kernel zu konfigurieren. Die anderen Dateien geben nur Informationen zu den aktuellen Einstellungen des Kernels aus.

Ein Wert in einer Datei in `/proc/sys` wird geändert, indem der neue Wert in diese Datei geschrieben wird. Zum Beispiel benutzt man, um den System Request Key in einem laufenden Kernel zu aktivieren, folgenden Befehl:

```
echo 1 > /proc/sys/kernel/sysrq
```

Dies ändert den Wert der Datei `sysrq` von `0` (off) auf `1` (on).

Einige Konfigurationsdateien in `/proc/sys/` enthalten mehr als einen Wert. Um neue Werte in solchen Dateien zu speichern, müssen Sie ein Leerzeichen zwischen jeden Wert setzen, den Sie übergeben. Sehen Sie die Anwendung mit dem Befehl `echo` hier:

```
echo 4 2 45 > /proc/sys/kernel/acct
```

Anmerkung

Konfigurationsänderungen, die Sie mit `echo` vornehmen gehen automatisch verloren, wenn das System neu gestartet wird. Um Ihre Konfigurations-Änderungen nach dem Booten wirksam werden zu lassen, lesen Sie bitte Abschnitt 5.4.

Das Verzeichnis `/proc/sys` enthält verschiedene Unterverzeichnisse, die verschiedene Bereiche des laufenden Kernel kontrollieren.

5.3.9.1. `/proc/sys/dev/`

Dieses Verzeichnis bietet Optionen für bestimmte Geräte im System an. Viele Systeme haben mindestens zwei Verzeichnisse: `cdrom` und `raid`, aber benutzerdefinierte Kernel können andere Verzeichnisse haben, wie z.B. `parport`, das es ermöglicht, den parallelen Port zwischen mehreren Treibern zu teilen.

Das `cdrom` Verzeichnis enthält eine Datei namens `info`, die einige wichtige CD-ROM-Parameter ausgibt:

```
CD-ROM information, Id: cdrom.c 3.12 2000/10/18

drive name:  hdc
drive speed:  32
drive # of slots: 1
Can close tray:  1
Can open tray:  1
```

```
Can lock tray:  1
Can change speed: 1
Can select disk: 0
Can read multisession: 1
Can read MCN:  1
Reports media changed: 1
Can play audio:  1
Can write CD-R:  0
Can write CD-RW: 0
Can read DVD:  0
Can write DVD-R: 0
Can write DVD-RAM: 0
```

Diese Datei kann benutzt werden, um die Fähigkeiten einer unbekannten CD-ROM herauszufinden. Wenn mehrere Laufwerke vorhanden sind, hat jedes Gerät seine eigene Informationsspalte.

Verschiedene Dateien in `/proc/sys/dev/cdrom`, wie z.B. `autoclose` und `checkmedia`, können benutzt werden, um das CD-ROM Laufwerk einzustellen. Mit dem Befehl `echo` können Sie ein Feature aktivieren oder deaktivieren.

Wenn RAID-Unterstützung in den Kernel integriert wurde, ist ein Verzeichnis `/proc/sys/dev/raid/` mit mindestens zwei Dateien vorhanden: `speed_limit_min` und `speed_limit_max`. Diese Einstellungen legen die Beschleunigung eines RAID Gerät für besonders I/O intensive Aufgaben, wie z.B. beim Synchronisieren von Festplatten, fest.

5.3.9.2. `/proc/sys/fs/`

Dieses Verzeichnis enthält eine Liste von Optionen und Informationen zu verschiedenen Einstellungen des Dateisystem, inklusive Quoten, Datei-Handles, Inoden und dentry-Informationen.

Das Verzeichnis `binfmt_misc` wirt benutzt, um Kernel Support für verschiedene Binär-Formate anzubieten.

Die wichtigen Dateien im Verzeichnis `/proc/sys/fs` sind:

- `dentry-state` — Zeigt den Status des Verzeichnis-Caches an. Diese Datei sieht so ähnlich wie diese aus:
  ```
  57411 52939 45 0 0 0
  ```
  Die erste Zahl zeigt die Gesamtzahl der Verzeichnis-Cache Einträge an, die zweite Zahl zeigt die Anzahl der nicht benutzten Einträgen an. Die dritte Zahl zeigt die Sekunden zwischem dem Löschen und dem erneuten Aufnehmen eines Verzeichnisses an. Die vierte misst die Seiten, die gerade vom System angefordert werden. Die letzten zwei Zahlen werden nicht benutzt und zeigen nur Nullen an.
- `dquot-nr` — Zeigt die maximale Anzahl von zwischengespeicherten Quoten-Einträgen an.
- `file-max` — Erlaubt es, die maximale Anzahl von Datei-Handles, die der Kernel zuweist, zu ändern. Diesen Wert zu ändern kann Fehler lösen, die beim Zuweisen von Datei-Handles entstehen können.
- `file-nr` — Zeigt die Anzahl zugewiesener, benutzter, und die maximale Anzahl der Datei-Handles an.
- `overflowgid` und `overflowuid` — Definiert die feste Benutzer- und Gruppen-ID, falls das System nur 16-bit Gruppen- und Benutzer-IDs unterstützt.
- `super-max` — Kontrolliert die maximal verfügbare Anzahl von Superblöcken.
- `super-nr` — Zeigt die aktuelle Anzahl der benutzten Superblöcke an.

5.3.9.3. `/proc/sys/kernel/`

Dieses Verzeichnis enthält eine Vielzahl von verschiedenen Konfigurationsdateien, die direkt die Kernelfunktion beeinflussen. Einige der wichtigsten Dateien sind unter anderem:

- `acct` — Kontrolliert die Aufhebung von Prozess Accounting, basierend auf der Prozentzahl des verfügbaren freien Speichers, der auf dem Dateisystem, das den Log enthält, verfügbar ist. Dieser Log sieht gewöhnlich so aus:
  ```
  4 2 30
  ```
  Der zweite Wert setzt den Schwellenwert des freien Speichers, wenn das Logging unterbrochen werden soll; der erste Wert hingegen zeigt den Wert an, wann das Logging wieder aufgenommen werden soll. Der dritte Wert zeigt das Intervall in Sekunden, in dem der Kernel das Dateisystem abfragt, um zu entscheiden, ob das Logging wieder aufgenommen oder unterbrochen werden soll.
- `cap-bound` — Kontrolliert die *Capability Bounding* Einstellungen. Diese bieten eine Liste von Möglichkeiten, die jeder Prozess auf dem System benutzten kann. Wenn eine Möglichkeit hier nicht aufgelistet ist, dann kann kein Prozess, egal mit welchen Privilegien, diese benutzen. Dies macht das System dadurch, dass bestimmte Dinge nicht ausgeführt werden können, sicherer (wenigstens nach einem bestimmten Punkt im Boot-Prozess nicht).

  Eine Liste gültiger Werte für diese virtuelle Datei finden Sie unter `/usr/src/linux-2.4/include/linux/capability.h`. Weitere Informationen zum Capability-Bounding finden Sie unter:
  `http://lwn.net/1999/1202/kernel.php3`
- `ctrl-alt-del` — Stellt ein, ob die Tastenkombination [Strg]-[Alt]-[Entf] den Rechner mittels des `init` Befehls (Wert `0`) neu startet oder einen sofortigen Neustart ohne Puffer-Synchronisation vornimmt; (Wert `1`).
- `domainname` — Erlaubt es, den Domainnamen des Systems zu konfigurieren, wie z.B. `example.com`.
- `hostname` — Erlaubt es, den Hostnamen des Systems zu konfigurieren, wie z.B. `www.example.com`.
- `hotplug` — Konfiguriert das Programm, das benutzt wird, wenn eine Konfigurationsänderung vom System erkannt wird. Dies wird vor allem mit dem USB und dem Cardbus PCI benutzt. Der Standardwert `/sbin/hotplug` sollte nicht geändert werden, außer wenn Sie ein neues Programm testen, dass diese Rolle ausfüllt.
- `modprobe` — Stellt den Speicherort des Programms ein, das Kernel-Module bei Bedarf lädt. Der Standardwert von `/sbin/modprobe` zeigt an, dass `kmod` dieses Programm aufruft, wenn ein Kernel Thread `kmod` aufruft, um ein Modul zu laden.
- `msgmax` — Setzt die maximale Größe von gesendeten Mitteilungen von einem Prozess zum anderen, wobei der Standardwert `8192` Bytes ist. Mit dem Erhöhen dieses Wertes sollten Sie vorsichtig sein, weil zwischengespeicherte Werte in nicht auslagerbarem Kernel-Speicher abgelegt werden, und jede Erhöhung in `msgmax` die RAM-Erfordernisse im System erhöhen.
- `msgmnb` — Setzt die maximale Anzahl von Bytes in einer einzelnen Mitteilungs-Queue. Standard ist hier `16384`.
- `msgmni` — Setzt die maximale Anzahl von Mitteilungs-Queue-IDs. Standard ist `16`.
- `osrelease` — Listet die Linux-Kernel Releasenummer auf. Diese Datei kann nur durch Neuübersetzung und Neukompilierung des Kernels verändert werden.
- `ostype` — Zeigt den Typ des Betriebssystems an. Diese Datei zeigt normalerweise `Linux` an; dieser Wert kann nur durch Ändern der Kernel-Quellen und Neukompilieren geändert werden.
- `overflowgid` und `overflowuid` — Definiert die feste Gruppen- und Benutzer-ID, die für Systemaufrufe bei Architekturen, die nur 16-bit Gruppen- und Benutzer-IDs unterstützen, benutzt werden.

- panic — Definiert die Anzahl von Sekunden, um die der Kernel den Neustart verschiebt, wenn ein "Kernel-Panik" auftritt. Dieser Wert steht normal auf 0, was einen automatischen Neustart nach einer "Kernel-Panik" deaktiviert.
- printk — Diese Datei kontrolliert eine Vielzahl von Einstellungen zum Anzeigen und Loggen von Fehlermitteilungen. Jede Fehlermeldung vom Kernel hat einen *loglevel*, der die Wichtigkeit der Mitteilung wiedergibt. Die Loglevel-Werte teilen sich wie folgt auf:
  - 0 — Ein Kernel Notfall. Das System ist nicht benutzbar.
  - 1 — Kernel-Alarm, es müssen sofort Gegenmaßnahmen eingeleitet werden.
  - 2 — Der Kernel ist in kritischem Zustand.
  - 3 — Allgemeiner Kernel-Fehler.
  - 4 — Allgemeine Kernel-Warnung.
  - 5 — Kernel-Mitteilung zu einem normalen, jedoch ernstzunehmendem Zustand.
  - 6 — Kernel Informations-Mitteilung.
  - 7 — Kernel Debugging-Mitteilung.

  Vier Werte finden sich in der Datei printk:
  ```
  6     4     1     7
  ```
  Jede dieser Werte definiert eine andere Regel zum Verarbeiten von Fehlermeldungen. Der erste Wert, *Konsolen-Loglevel* genannt, definiert die niedrigste Priorität von Mitteilungen, die auf die Konsole ausgegeben werden (je niedriger die Priorität, desto höher die Loglevel-Nummer). Der zweite Wert setzt den Standart-Loglevel für Mitteilungen, welche keinen Loglevel gesetzt haben. Der dritte Wert setzt den niedrigsten Loglevel Konfigurationswert für den Konsolen Loglevel. Der letzte Wert setzt den Standardwert für den Konsolen-Loglevel.
- random/ Verzeichnis — Listet eine Anzahl von Werten, die zum Erzeugen von Zufallszahlen im Kernel verwendet werden.
- rtsig-max — Konfiguriert die maximale Anzahl an POSIX-Echtzeitsignalen, die das System gespeichert haben kann. Der Standardwert ist: 1024.
- rtsig-nr — Die aktuelle Anzahl von POSIX-Echzeitsignalen, die zur Zeit vom Kernel abgearbeitet werden.
- sem — Diese Datei konfiguriert die Semaphore-Einstellungen im Kernel. Eine *semaphore* ist ein System V IPC-Objekt, das benutzt wird, um den Einsatz eines bestimmten Prozesses zu überwachen.
- shmall — Zeigt den Gesamtwert des gemeinsam verwendeten Speichers in Bytes an, der gleichzeitig im System benutzt werden kann. Dieser Wert ist normalerweise: 2097152.
- shmmax — Stellt die größte Speichersegmentgröße in Bytes ein, die vom Kernel erlaubt wird. Dieser Wert ist normalerweise 33554432. Der Kernel unterstützt allerdings viel größere Werte.
- shmmni — Stellt die maximale Anzahl von gemeisam genutzten Speichersegmenten für das ganze System ein. Dieser Wert hat den Standardwert 4096.
- sysrq — Aktiviert den System-Request-Key, wenn dieser Wert nicht auf das standardmäßige 0 gesetzt ist.

  Der Sinn des System-Request-Key ist es, Ihnen zu erlauben, dem Kernel direkte Anweisungen mit einer simplen Tastenkombination zu geben, um den Rechner z.B. direkt herunter zu fahren, das System neu zu starten, alle Dateisystempuffer zu schreiben oder wichtige Informationen auf Ihre Konsole zu schreiben. Um den System-Request-Key zu aktivieren, drücken Sie [Alt]-[SysRq]-[*<system request code>*]. Ersetzen Sie *<system request code>* mit einem der folgenden System-Request-Codes:

- `r` — Deaktiviert Raw-Mode für die Tastatur und setzt dieses auf XLATE (ein eingeschränkterer Tastaturmodus, der die Tasten [Alt], [Ctrl] oder [Shift] für keine der Keys erkennt).
- `k` — Vernichtet alle Prozesse, die in der virtuellen Konsole aktiv sind. Auch *Secure Access Key* (*SAK*) genannt, wird dieser oft verwendet, um zu prüfen, dass der Login-Prompt von `init` gestartet wird, und nicht eine trojanische Kopie, die darauf aus ist Benutzernamen und Passwörter zu sammeln.
- `b` — Startet den Kernel neu, ohne dabei zuerst einen Unmount auf Dateisysteme durchzuführen, oder einen Sync zu Platten, die an das System angebunden sind.
- `c` — Verursacht einen Absturz des Systems, ohne dabei zuerst einen Unmount auf Dateisysteme durchzuführen, oder einen Sync zu Platten, die an das System angebunden sind.
- `o` — Fährt das System herunter.
- `s` — Versucht einen Sync auf Platten, die an das System angebunden sind.
- `u` — Versucht einen Unmount und dann einen Mount in Read-Only für alle Dateisysteme.
- `p` — Gibt alle Flags und Register zur Konsole aus.
- `t` — Gibt eine Liste der Prozesse zur Konsole aus.
- `m` — Gibt Speicherstatistiken zur Konsole aus.
- `0` bis `9` — Setzt den Log-Level für die Konsole.
- `e` — Vernichtet alle Prozesse, ausser `init`, der SIGTERM verwendet.
- `i` — Vernichtet alle Prozesse, ausser `init`, der SIGKILL verwendet.
- `l` — Vernichtet alle Prozesse, die SIGKILL verwenden (einschließlich `init`). Das System ist nach Ausführen dieses System-Request-Key-Code unbrauchbar.
- `h` — Gibt Hilfetext aus.

Dieses Feature ist sehr nützlich bei der Verwendung eines Entwicklungskernel oder wenn ein Einfrieren des Systems auftritt.

Achtung

Das System-Request-Key Feature wird als Sicherheitsrisiko angesehen, da eine unbewachte Konsole einem Angreifer Zugriff zum System ermöglichen könnte. Aus diesem Grund ist es standardmäßig ausgeschaltet.

Weitere Informationen zum System-Request-Key finden Sie unter `/usr/src/linux-2.4/Documentation/sysrq.txt`.

- `sysrq-key` — Bestimmt den Key-Code für den System-Request-Key (standardmäßige `84`).
- `sysrq-sticky` — Bestimmt, ob der System-Request-Key eine "chorded" Tastenkombination ist. Die angenommenen Werte sind wie Folgt:
  - `0` — [Alt]-[SysRq] und der System-Request-Code müssen gleichzeitig gedrückt werden. Dies ist die Vorgabe.
  - `1` — [Alt]-[SysRq] müssen gleichzeitig gedrückt werden, der System-Request-Code kann jedoch jederzeit, innerhalb der in `/proc/sys/kernel/sysrq-timer` angegebenen Sekunden gedrückt werden.
- `sysrq-timer` — Gibt die Anzahl von Sekunden an, die Ablaufen können, bevor der System-Request-Code gedrückt werden muss. Der Standardwert ist `10`.
- `tainted` — Zeigt an, ob ein non-GPL Modul geladen ist.
  - `0` — Keine non-GPL Module sind geladen.

- 1 — Wenigstens ein Modul ohne GPL-Lizenz (einschließlich Module ohne Lizenz) ist geladen.
- 2 — Zumindest ein Modul wurde mit dem Befehl insmod -f zwangsweise geladen.

- threads-max — Stellt die maximale Anzahl von Threads, die vom Kernel genutzt werden können, ein. Standardwert: 4095.
- version — Zeigt Datum und Zeit der letzten Kernel-Kompilierung an. Das erste Feld in dieser Datei, wie z.B. #3 zeigt an, wie oft ein Kernel aus den Quellen neukompiliert wurde.

5.3.9.4. /proc/sys/net/

Dieses Verzeichnis enthält Unterverzeichnisse über verschiedene Netzwerk-Themen. Verschiedene Konfigurationen zur Kernel-Kompilierung erzeugen hier verschiedene Verzeichnisse, wie z.B. appletalk, ethernet, ipv4, ipx und ipv6. In diesen Verzeichnissen können Sie verschiedene Netzwerk-Einstellungen für diese Konfiguration am laufenden System ändern.

Aufgrund der vielfältigen Netzwerk-Optionen, die in Linux verwendet werden können, werden wir nur die wichtigsten Verzeichnisse in /proc/sys/net/ vorstellen.

Das Verzeichnis /proc/sys/net/core/ enthält eine Vielzahl von Einstellungen, die die Interaktion zwischen Kernel und Netzwerkschichten beeinflussen. Die wichtigsten Dateien sind hier:

- message_burst — Die Anzahl Zehntelsekunden, die benötigt werden, um eine neue Warnungsmitteilung zu schreiben. Das wird benutzt, um *Denial of Service* (*DoS*) Angriffe zu vermeiden; die Standardeinstellung ist: 50.
- message_cost — Wird auch verwendet, um DoS Angriffe zu vermeiden, indem ein Cost-Faktor auf jede Warnung gesetzt wird. Je höher der Wert dieser Datei (Standard ist 5), desto eher wird die Warnung ignoriert. Diese Einstellung wird im Bezug zu DoS-Angriffen verwendet.

  Eine DoS-Attacke bedeutet, dass ein Angreifer Ihr System mit Anfragen überhäuft, die Fehler erzeugen und ihre Diskpartitionen mit Logdateien füllen oder Ihre Systemressourcen zum Fehlerloggen verbrauchen. Die Einstellungen in message_burst und message_cost sind dazu da, ein Gleichgewicht zwischen gutem Logging und einem geringen Risiko einzustellen.
- netdev_max_backlog — Setzt die maximale Nummer von Paketen, die in die Warteschlange gestellt werden, wenn eine Schnittstelle Pakete schneller empfängt, als der Kernel diese verarbeiten kann. Der Standardwert hier ist: 300.
- optmem_max — Konfiguriert die maximale zusätzliche Puffergröße pro Socket.
- rmem_default — Setzt die Standardgröße für den Empfangspuffer in Byte.
- rmem_max — Setzt die Maximalgröße des Empfangspuffers in Byte.
- wmem_default — Setzt die Standardgröße für den Sendepuffer in Byte.
- wmem_max — Setzt die Maximalgröße für den Sendepuffer in Byte.

Das Verzeichnis /proc/sys/net/ipv4/ enthält weitere Netzwerkeinstellungen. Viele dieser Einstellungen, die zusammen verwendet werden, sind sehr hilfreich bei der Verhinderung von Angriffen auf das System oder bei der Verwendung des Systems als Router.

Achtung

Eine irrtümliche Änderung dieser Dateien kann die Netzwerkverbindungen beeinträchtigen.

Folgend ist eine Liste einiger der wichtigeren Dateien im Verzeichnis /proc/sys/net/ipv4/:

- `icmp_destunreach_rate`, `icmp_echoreply_rate`, `icmp_paramprob_rate` und `icmp_timeexeed_rate` — Stellt die maximale ICMP Send-Paket Rate in 1/100 Sekunden an Hosts unter verschiedenen Bedingungen ein. Eine Einstellung von `0` entfernt alle Verzögerungen und sollte nicht eingestellt werden.
- `icmp_echo_ignore_all` und `icmp_echo_ignore_broadcasts` — Erlaubt dem Kernel, ICMP ECHO Pakete von allen Hosts oder nur solche von Broadcast- oder Multicast-Adressen zu ignorieren. Eine `0` erlaubt dem Kernel zu antworten, eine `1` ignoriert diese Pakete.
- `ip_default_ttl` — Stellt die Standard *Time To Live (TTL)* ein, die die Anzahl von Sprüngen limitiert, bevor ein Paket sein Ziel erreicht. Eine Erhöhung dieses Wertes kann unter Umständen die Systemleistung beeinträchtigen.
- `ip_forward` — Erlaubt Schnittstellen im System, Pakete zu einer anderen weiterzuleiten. Standardmäßig ist diese Datei auf `0` gesetzt, um das Weiterleiten auszuschalten. Eine `1` aktiviert die Paketweiterleitung.
- `ip_local_port_range` — Legt die Ports fest, die von TCP oder UDP benutzt werden, wenn ein lokaler Port gebraucht wird. Die erste Zahl ist der niedrigste Port und die zweite Zahl steht für den höchsten benutzten Port. Jedes System, für das erwartet wird, dass es mehr als die Standard Ports 1024 bis 4999 benötigt, sollte die Werte 32768 bis 61000 verwenden.
- `tcp_syn_retries` — Bietet eine Grenze dafür an, wie oft Ihr System ein SYN Paket versucht zu übertragen, wenn eine Verbindung versucht wird.
- `tcp_retries1` — Stellt die Anzahl von zugelassenen Neu-Übertragungen ein, wenn versucht wird einer eingehenden Verbindung zu antworten. Standardwert ist hier `3`.
- `tcp_retries2` — Stellt die Anzahl von erlaubten Neu-Übertragungen von TCP Paketen ein. Standardwert ist `15`.

Die Datei `/usr/src/linux-2.4/Documentation/networking/ip-sysctl.txt` enthält eine komplette Liste der im Verzeichnis `/proc/sys/net/ipv4/` verfügbaren Dateien und Optionen.

Eine Anzahl anderer Verzeichnisse in `/proc/sys/net/ipv4/` behandeln spezifische Inhalte. Das Verzeichnis `/proc/sys/net/ipv4/conf/` erlaubt jeder der Systemschnittstellen eine unterschiedliche Konfiguration und lässt Standard Werte für nicht-konfigurierte Schnittstellen (im Unterverzeichnis `/proc/sys/net/ipv4/conf/default/`), und Einstellungen, die alle anderen Konfigurationen überschreiben (im Verzeichnis `/proc/sys/net/ipv4/conf/all/`), zu.

Um Verbindungen zwischen direkten Nachbarn (hier jedes andere System, das direkt an das System angeschlossen ist) zu überwachen, bietet das Verzeichnis `/proc/sys/net/ipv4/neigh/` (steht für neighbors) spezielle Konfigurationen für jede Schnittstelle an. Das erlaubt Ihnen, Systeme denen Sie aufgrund ihrer örtlichen Nähe mehr vertrauen, anders zu behandeln. Es macht es gleichzeitig aber auch möglich, örtlich entfernte Systeme mit festen Regeln zu belegen.

Das Routen über IPV4 besitzt auch ein eigenes Verzeichnis `/proc/sys/net/ipv4/route/`. Im Gegensatz zu `conf` und `neigh`, enthält das `/proc/sys/net/ipv4/route/` Verzeichnis Spezifikationen, die das Routing auf allen Systemschnittstellen beeinflusst. Viele dieser Einstellungen, wie z.B. `max_size`, `max_delay` und `min_delay`, hängen mit der Einstellung des Routing Caches zusammen. Um den Routing Cache zu löschen, schreiben Sie einen beliebigen Inhalt in die Datei `flush`.

Zusätzliche Informationen über diese Verzeichnisse und die möglichen Werte zur Konfiguration finden Sie unter:

```
/usr/src/linux-2.4/Documentation/filesystems/proc.txt
```

5.3.9.5. `/proc/sys/vm/`

Dieses Verzeichnis erleichtert die Konfiguration des virtuellen Speicher-Subsystems des Linux Kernels (VM). Der Kernel macht ausgiebigen und intelligenten Gebrauch von virtuellem Speicher, der

auch Swap-Speicher genannt wird.

Die folgenden Dateien findet man normalerweise im Verzeichnis `/proc/sys/vm/`:

- `bdflush` — Setzt verschiedene Werte, in Bezug auf den `bdflush` Kernel-Daemon.
- `kswapd` — Stellt verschiedene Werte, in Zusammenhang mit dem Kernel-Swap-Out-Daemon ein; `kswapd`. Diese Datei hat drei Werte:
  ```
  512 32 8
  ```
  Der erste Wert setzt die maximale Anzahl von Seiten, die `kswapd` in einem Versuch zu löschen versucht. Je größer diese Zahl, desto schneller kann der Kernel auf freie Seiten zurückgreifen. Der zweite Wert setzt die minimale Anzahl von Versuchen, die `kswapd` versucht, eine Seite zu löschen. Der dritte Wert setzt die Anzahl von Seiten, die `kswapd` in einem Versuch zu schreiben versucht. Ein richtiges Einstellen des letzten Wertes kann die Systemleistung auf Kosten einer Menge Swap-Platzes erhöhen, indem der Kernel Seiten in großen Blöcken schreibt und dabei die Anzahl der Plattenzugriffe verringert.
- `max_map_count` — Konfiguriert die maximale Anzahl von Speicher-Map-Bereichen, die ein Prozess haben darf. In den meisten Fällen ist ein Standardwert von `65536` angemessen.
- `hugetlb_pool` — Gibt die Größe der Hugepages — große, physisch kontinuierliche Speicherseiten — in Megabytes an. Diese Seiten können verwendet werden, um große TLB virtuelle Speicher-Abbildungen zu erzeugen, die für RAM-intensive Datenbankapplikationen nützlich sind. TLB ist ein spezielle in-CPU Cache, der für solche virtuellen Speicher-Abbildungen entwickelt wurde.

  Obwohl dieses Feature zur Laufzeit geändert werden kann, ist dieses sensitiv im Bezug zu Fragmetierung, wenn der Pool erweitert wird während das Feld `MemFree` von `/proc/meminfo` niedrig ist. Aus diesem Grund kann es wichtig sein, neue Einstellungen in `/etc/sysctl.conf` vorzunehmen und neu zu starten. Siehe Abschnitt 5.4 für Informationen zu `sysctl`.

  Siehe `/usr/src/linux-2.4/Documentation/vm/hugetlbpage.txt` für weitere Information zur Konfiguration von hugepages.

  Wichtig

  Obwohl in `hugetlbpage.txt` erwähnt, ist die Datei `/proc/sys/vm/nr_hugepages` *nicht* in Red Hat Enterprise Linux enthalten. `hugetlb_pool` sollte anstelle verwendet werden, um die Anzahl der für das System verfügbaren Hugepages zu konfigurieren. Es ist auch wichtig zu beachten, dass `nr_hugepages` hugepage-Einheiten verwendet, während `hugetlb_pool` konfiguriert hugepages in Megabytes.

- `overcommit_memory` — Konfiguriert die Bedingungen, unter denen große Speicheranforderungen akzeptiert oder abgelehnt werden. Die folgenden drei Modi sind verfügbar:
  - `0` — Der Kernel führt ein heuristisches "memory overcommit handling" durch und schätzt einen verfügbaren Speicherumfang und lässt Anfragen scheitern, die eindeutig ungültig sind. Da bei der Speicherzuordnung eher ein heuristischer als ein genauer Algorithmus verwendet wird, kann es manchmal zu einer Überlastung des Systems kommen. Dies ist die Vorgabe.
  - `1` — Der Kernel führt kein "memory overcommit handling" durch. Dies erhöht die Wahrscheinlichkeit einer Systemüberlastung. Das gleiche gilt für die Durchführung von speicherintensiven Aufgaben (wie die, die von einigen wissenschaftlichen Softwareprogrammen verwendet werden).
  - `2` — Der Kernel lässt Anfragen scheitern, die Größen des gesamten Swap, plus dem physischem RAM, dass in `/proc/sys/vm/overcommit_ratio` angegeben ist hinzufügen. Diese Einstellung ist am Besten für die, die weniger "memory overcommitment" riskieren wollen.

Anmerkung

Diese Einstellung ist nur für Systeme empfohlen, deren Swap größer als deren physischer Speicher ist.

- `overcommit_ratio` — Gibt den Prozentanteil an physischem RAM an, der berücksichtigt wird, wenn `/proc/sys/vm/overcommit_memory` auf `2` gesetzt ist. Der Standardwert ist `50`.
- `pagecache` — Erlaubt es Ihnen, den Anteil, in Prozent, des System-Speichers einzustellen, der als Page-Cache verwendet wird. Eine typische Ausgabe dieser Datei sieht wie folgt aus:

  ```
  1       15      100
  ```

  Der erste Wert setzt den minimalen Speicher, der als Page-Cache-Speicher verwendet wird. Der mittlere Wert setzt den Prozentsatz von Systemspeicher, der als Puffer und Page-Cache verwendet wird, ab dem das Memory Management anfängt, Puffer mehr als andere Speichertypen zu löschen, um Speichermangel auszugleichen. Der letzte Wert setzt den maximalen Speicher, der als Pufferspeicher verwendet wird, ist allerdings noch nicht implementiert.
- `page-cluster` — Stellt die Anzahl von Seiten, die auf einmal gelesen werden sollen, ein. Der Standardwert `3`, der sich eigentlich auf 16 Seiten bezieht, reicht für die meisten Systeme aus.
- `pagetable_cache` — Stellt die Anzahl von Seiten ein, die auf Pro-Prozessor Basis zwischengespeichert werden, ein. Der erste und zweite Wert beziehen sich auf die minmale und die maximale Anzahl von Seitentabellen.

Zusätzliche Informationen hierzu finden Sie in `/usr/src/linux-2.4/Documentation/sysctl/vm.txt`.

5.3.10. `/proc/sysvipc/`

Dieses Verzeichnis enthält Informationen über die System V IPC-Ressourcen. Die Dateien in diesem Verzeichnis hängen mit den System V IPC-Aufrufen zusammen (`msg`), Semaphores (`sem`) und gemeinsam benutzter Speicher (`shm`).

5.3.11. `/proc/tty/`

Dieses Verzeichnis enthält Informationen über die verfügbaren und zur Zeit benutzten TTY-Geräte im System. Früher *teletype device* genannt, werden heute alle Buchstaben-orientierten Daten Terminals als TTY-Geräte bezeichnet.

Unter Linux gibt es drei verschiedene Arten von TTY-Geräten. *Serielle Geräte* werden mit seriellen Verbindungen benutzt, wie z.B. mit Modems oder seriellen Kabeln. *Virtuelle Terminals* erzeugen die normalen Konsolenverbindungen, wie die virtuellen Konsolen, die verfügbar sind, wenn Sie [Alt]-[<F-key>] auf einer Systemkonsole drücken. *Pseudo Terminals* erzeugen eine zwei-Wege Kommunikation, die von einigen höherrangigen Applikationen, wie z.B. XFree86 verwendet werden. Die Datei `drivers` enthält eine Liste der TTY-Geräte, die zur Zeit benutzt werden:

```
serial               /dev/cua        5  64-127 serial:callout
serial               /dev/ttyS       4  64-127 serial
pty_slave            /dev/pts      136   0-255 pty:slave
pty_master           /dev/ptm      128   0-255 pty:master
pty_slave            /dev/ttyp       3   0-255 pty:slave
pty_master           /dev/pty        2   0-255 pty:master
/dev/vc/0            /dev/vc/0       4       0 system:vtmaster
```

```
/dev/ptmx            /dev/ptmx       5       2 system
/dev/console         /dev/console    5       1 system:console
/dev/tty             /dev/tty        5       0 system:/dev/tty
unknown              /dev/vc/%d      4    1-63 console
```

Die Datei `/proc/tty/driver/serial` listet die Nutzungs-Statistik und den Status jedes der seriellen TTY-Geräte auf.

Damit TTY-Geräte ähnlich wie Netzwerk-Geräte benutzt werden können, stellt der Kernel *line discipline* für das Gerät ein. Das erlaubt dem Treiber, einen bestimmten Headertyp mit jedem Datenblock, der über das Gerät geht, zu transferieren; dieser Header macht das Paket zu einem Paket in einem Stream. SLIP und PPP sind allgemein bekannte Line Disciplines und werden vor allem benutzt, um Systeme über eine serielle Verbindung zu koppeln.

Registrierte Line Disciplines werden in der Datei `ldiscs` gespeichert; detaillierte Informationen finden Sie im Verzeichnis `ldisc/`.

5.4. Benutzen von `sysctl`

Der Befehl `/sbin/sysctl` wird zum Betrachten, Setzen und Automatisieren von Kerneleinstellungen im Verzeichnis `/proc/sys` verwendet.

Um einen schnellen Überblick über alle konfigurierbaren Einstellungen im Verzeichnis `/proc/sys/` zu bekommen, geben Sie den Befehl `/sbin/sysctl -a` als root ein. Dies gibt eine lange, umfassende Liste aus; ein kleiner Teil dieser Liste könnte z.B. so aussehen:

```
net.ipv4.route.min_delay = 2
kernel.sysrq = 0
kernel.sem = 250     32000     32     128
```

Das ist im Prinzip diesselbe Information, die Sie auch sähen, wenn Sie jede Datei einzeln betrachteten. Der einzige Unterschied ist der Ort der Datei. Die Datei `/proc/sys/net/ipv4/route/min_delay` wird durch `net.ipv4.route.min_delay` angesprochen, die Schrägstriche im Verzeichnis werden durch Punkte ersetzt, und der`proc.sys` Teil wird angenommen.

Der Befehl `sysctl` kann anstelle von `echo` für das Zuweisen von Werten zu schreibbaren Dateien im Verzeichnis `/proc/sys/` verwendet werden. Statt diesen Befehl zu verwenden:

```
echo 1 > /proc/sys/kernel/sysrq
```

Der entsprechende `sysctl`-Befehl ist Folgender:

```
sysctl -w kernel.sysrq="1"
kernel.sysrq = 1
```

Auch wenn das schnelle Setzen von Werten, wie bei diesem in `/proc/sys/` nützlich zum Testen ist, funktioniert das nicht gut auf einem Produktionssystem, weil alle Einstellungen aus `/proc/sys/` bei einem Neustart verloren gehen. Um permanente Einstellungen zu sichern, fügen Sie diese zu der Datei `/etc/sysctl.conf` hinzu.

Jedes Mal, wenn das System gestartet wird, wird das Skript `/etc/rc.d/rc.sysinit` von `init` aufgerufen. Dieses Skript enthält einen Befehl um `sysctl` auszuführen und verwendet `/etc/sysctl.conf` zur Vorgabe der Werte, die an den Kernel gegegeben wurden. Alle Werte, die zu `/etc/sysctl.conf` hinzugeführt wurden, werden nach jedem Neustart aktiviert.

5.5. Zusätzliche Ressourcen

Nachstehend finden Sie zusätzliche Quellenangaben für Informationen über das Dateisystem /proc.

5.5.1. Installierte Dokumentation

Eine Auswahl der besten Dokumentation zum proc-Dateisystem ist standardmäßig auf dem System installiert.

- /usr/src/linux-2.4/Documentation/filesystems/proc.txt — Enthält bestimmte, jedoch eingeschränkte Dokumentation zu den Aspekten von /proc.
- /usr/src/linux-2.4/Documentation/sysrq.txt — Ein Überblick über die System Request Key Optionen.
- /usr/src/linux-2.4/Documentation/sysctl/ — Ein Verzeichnis, dass eine Vielzahl von Tips zu sysctl enthält, inklusive Optionen, die den Kernel angehen (kernel.txt), zu den Dateisystemen (fs.txt) und zum virtuellen Speicher (vm.txt).
- /usr/src/linux-2.4/Documentation/networking/ip-sysctl.txt — Ein detallierter Überblick auf verschiedene IP-Netzwerk Optionen.
- /usr/src/linux-2.4/ — Die vielleicht wichtigste Informationsquelle zu /proc/ ist der Sourcecode des Linux-Kernels. Wenn Sie das RPM Paket kernel-source installiert haben, finden Sie diesen im Verzeichnis /usr/src/linux-2.4/.

5.5.2. Hilfreiche Websites

- http://www.linuxhq.com/ — Diese Seite wartet eine komplette Datenbank mit Quellcode, Patches und Dokumentation für verschiedene Versionen des Linux-Kernels.

redhat

Kapitel 6.

Benutzer und Gruppen

Die *Benutzer*- und *Gruppen*-Kontrolle ist ein grundlegendes Element der Red Hat Enterprise Linux-Systemadministration.

Benutzer können sowohl Personen sein, d.h. Accounts, die an einen bestimmten Benutzer gebunden sind, als auch Accounts, die für bestimmte Anwendungen gedacht sind.

Gruppen sind der logische Ausdruck einer Zusammenfassung von Benutzern zu einem bestimmten Zweck. Alle Benutzer in der selben Gruppe, können Dateien dieser Gruppe Lesen, Schreiben und Ausführen.

Jeder Benutzer und jede Gruppe hat eine eindeutige numerische Identifikationsnummer, *Benutzer-ID* (*UID*) bzw *Gruppen-ID* (*GID*) genannt.

Der Benutzer, der eine Datei erstellt, wird als Besitzer und Gruppenbesitzer eingesetzt. Darüber hinaus werden dem Dateibesitzer, der Gruppe und allen anderen eigene Berechtigungen zum Lesen, Schreiben und Ausführen zugewiesen. Der Besitzer einer Datei kann nur durch den Root-Benutzer geändert werden. Die Gruppe, zu der eine Datei gehört, kann nur durch den Root oder durch den Besitzer der Datei geändert werden, wenn Letzterer Teil der Gruppe ist, die zur Datei hinzugefügt wird. Die Zugriffsberechtigungen für diese Datei können sowohl vom Root-Benutzer als auch vom Besitzer der Datei geändert werden.

Red Hat Enterprise Linux unterstützt *Zugangskontrolllisten* (*ACLs*) für Dateien und Verzeichnisse, die gestatten, dass gewisse Benutzer außerhalb des Besitzers eingerichtet werden können. Für weitere Informationen über die Verwendung von ACLs siehe Kapitel*Access Control Lists* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Eine gute Verwaltung von Benutzern und Gruppen sowie eine effektive Verwaltung der Dateiberechtigungen gehören zu den wichtigsten Aufgaben eines System-Administrators. Für einen detaillierten Überblick der Strategien zum Management von Benutzern und Gruppen, siehe Kapitel *Managing User Accounts and Resource Access* im *Red Hat Enterprise Linux Introduction to System Administration*.

6.1. Tools zum Management von Benutzern und Gruppen

Die Verwaltung von Benutzern und Gruppen kann sehr langwierig sein, Red Hat Enterprise Linux liefert allerdings ein paar Tools und Konventionen, die diese Aufgabe erleichtern sollen.

Der einfachste Weg, Benutzer und Gruppen zu verwalten, ist mit Hilfe der grafischen Anwendung **User Manager** (`redhat-config-users`). Für mehr Informationen zu **User Manager**, siehe Kapitel *Benutzer- und Gruppenkonfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Auch können die folgenden Befehlszeilentools zum Verwalten von Benutzern und Gruppen verwendet werden:

- `useradd`, `usermod`, und `userdel` — Methoden des Industriestandards zum Hinzufügen, Löschen und Ändern von Benutzeraccounts.
- `groupadd`, `groupmod`, und `groupdel` — Methoden des Industriestandards zum Hinzufügen, Löschen und Ändern von Gruppen.
- `gpasswd` — Methode des Industriestandards zum Verwalten der Datei `/etc/group`.
- `pwck`, `grpck` — Tools zum Überprüfen von Passwort, Gruppe und zugehörigen Schattendateien.

- `pwconv`, `pwunconv` — Tools für die Konvertierung von Passwörtern zu Shadow-Passwörtern und wieder zurück zu Standard-Passwörtern.

Einen Überblick über das Verwalten von Benutzern und Gruppen finden Sie im *Red Hat Enterprise Linux Introduction to System Administration*. Für eine detaillierte Beschreibung von Befehlszeilentools zur Verwaltung von Benutzern und Gruppen siehe Kapitel *Benutzer- und Gruppenkonfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

6.2. Standardbenutzer

Tabelle 6-1 zeigt die Standardbenutzer, die während des Installationsvorgangs in der Datei `/etc/passwd` eingerichtet werden. Die Gruppen-ID (GID) in der Tabelle gibt die *Hauptgruppe* des Benutzers an. Eine Auflistung der Standardgruppen finden Sie in Abschnitt 6.3.

Benutzer	UID	GID	Benutzer-Verzeichnis	Shell
root	0	0	`/root`	`/bin/bash`
bin	1	1	`/bin`	`/sbin/nologin`
daemon	2	2	`/sbin`	`/sbin/nologin`
adm	3	4	`/var/adm`	`/sbin/nologin`
lp	4	7	`/var/spool/lpd`	`/sbin/nologin`
sync	5	0	`/sbin`	`/bin/sync`
shutdown	6	0	`/sbin`	`/sbin/shutdown`
halt	7	0	`/sbin`	`/sbin/halt`
mail	8	12	`/var/spool/mail`	`/sbin/nologin`
news	9	13	`/var/spool/news`	
uucp	10	14	`/var/spool/uucp`	`/sbin/nologin`
operator	11	0	`/root`	`/sbin/nologin`
games	12	100	`/usr/games`	`/sbin/nologin`
gopher	13	30	`/usr/lib/gopher-data`	`/sbin/nologin`
ftp	14	50	`/var/ftp`	`/sbin/nologin`
nobody	99	99	`/`	`/sbin/nologin`
rpm	37	37	`/var/lib/rpm`	`/bin/bash`
vcsa	69	69	`/dev`	`/sbin/nologin`
ntp	38	38	`/etc/ntp`	`/sbin/nologin`
canna	39	39	`/var/lib/canna`	`/sbin/nologin`
nscd	28	28	`/`	`/bin/false`
rpc	32	32	`/`	`/sbin/nologin`
postfix	89	89	`/var/spool/postfix`	`/bin/true`

Benutzer	UID	GID	Benutzer-Verzeichnis	Shell
named	25	25	/var/named	/bin/false
amanda	33	6	var/lib/amanda/	/bin/bash
postgres	26	26	/var/lib/pgsql	/bin/bash
sshd	74	74	/var/empty/sshd	/sbin/nologin
rpcuser	29	29	/var/lib/nfs	/sbin/nologin
nsfnobody	65534	65534	/var/lib/nfs	/sbin/nologin
pvm	24	24	/usr/share/pvm3	/bin/bash
apache	48	48	/var/www	/bin/false
xfs	43	43	/etc/X11/fs	/sbin/nologin
desktop	80	80	/var/lib/menu/kde	/sbin/nologin
gdm	42	42	/var/gdm	/sbin/nologin
mysql	27	27	/var/lib/mysql	/bin/bash
webalizer	67	67	/var/www/html/usage	/sbin/nologin
mailnull	47	47	/var/spool/mqueue	/sbin/nologin
smmsp	51	51	/var/spool/mqueue	/sbin/nologin
squid	23	23	/var/spool/squid	/dev/null
ldap	55	55	/var/lib/ldap	/bin/false
netdump	34	34	/var/crash	/bin/bash
pcap	77	77	/var/arpwatch	/sbin/nologin
radvd	75	75	/	/bin/false
Quagga	92	92	/var/run/quagga	/bin/false
wnn	49	49	/var/lib/wnn	/bin/bash

Tabelle 6-1. Standardbenutzer

6.3. Standardgruppen

In Tabelle 6-2 sind die Standardgruppen aufgeführt, die von einer "Alles"-Installation konfiguriert werden. Die Gruppen werden in der Datei `/etc/group` gespeichert.

Gruppe	GID	Mitglieder
root	0	root
bin	1	root, bin, daemon
daemon	2	root, bin, daemon
sys	3	root, bin, adm
adm	4	root, adm, daemon
tty	5	

Gruppe	GID	Mitglieder
disk	6	root
lp	7	daemon, lp
mem	8	
kmem	9	
wheel	10	root
mail	12	Mail, Postfix
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	
ftp	50	
lock	54	
nobody	99	
Benutzer	100	
rpm	37	
utmp	22	
floppy	19	
vcsa	69	
ntp	38	
canna	39	
nscd	28	
rpc	32	
postdrop	90	
postfix	89	
named	25	
postgres	26	
sshd	74	
rpcuser	29	
nfsnobody	65534	
pvm	24	
apache	48	
xfs	43	
desktop	80	

Gruppe	GID	Mitglieder
gdm	42	
mysql	27	
webalizer	67	
mailnull	47	
smmsp	51	
squid	23	
ldap	55	
netdump	34	
pcap	77	
Quaggavty	101	
Quagga	92	
radvd	75	
slocate	21	
wnn	49	

Tabelle 6-2. Standardgruppen

6.4. Benutzereigene Gruppen

Red Hat Enterprise Linux verwendet ein Schema für *benutzereigene Gruppen* (*UPG*), das die Verwaltung von UNIX-Gruppen vereinfacht.

Eine UPG wird erzeugt, wenn ein neuer Benutzer zum System hinzugefügt wird. UPGs haben den selben Namen wie der Benutzer, für welchen diese erzeugt wurden und lediglich dieser Benutzer ist Mitglied der Gruppe.

UGP ermöglicht das sichere Einstellen von Standard-Genehmigungen für eine neu erstellte Datei oder ein Verzeichnis, die/das sowohl dem Benutzer als auch *der Gruppe dieses Benutzers* gestatten, Veränderungen an der Datei oder am Verzeichnis vorzunehmen.

Die Einstellung, die festlegt, welche Rechte einer neu erzeugten Datei oder einem Verzeichnis zugewiesen werden, wird *umask* gennannt und ist in der Datei `/etc/bashrc` enthalten. Auf UNIX-Systemen ist die umask, traditionell, 022, was andere Benutzer *und andere Mitglieder der Gruppe des Benutzers* davon abhält, diese Dateien zu ändern. Da jeder Benutzer ihre/seine eigene private Gruppe im UPG Schema hat, ist dieser "Gruppenschutz" nicht notwendig.

6.4.1. Gruppenverzeichnisse

Viele IT-Organisationen ziehen es vor, eine Gruppe für jedes größere Projekt zu erstellen und dann dieser Gruppe Mitarbeiter zuzuweisen, wenn sie auf die Dateien des Projekts zugreifen müssen. Bei dieser traditionellen Methode ist das Management von solchen Dateien schwierig, denn wennjemand eine Datei erstellt, ist sie mit der Hauptgruppe des Benutzers assoziiert. Wenn eine einzelne Person an mehreren Projekten gleichzeitig arbeitet, ist es schwierig, die richtigen Dateien der richtigen Gruppe zuzuweisen. Unter Verwendung des UPG Schemas werden Gruppen automatisch Dateien zugewiesen, die in Verzeichnissen erstellt werden, die das *setgid*Bit eingestellt haben. Dies vereinfacht das Management von Gruppenprojekten, die sich ein gemeinsames Verzeichnis teilen, erheblich. Alle Dateien,

die ein Benutzer innerhalb des Verzeichnisses erstellt, gehören der Gruppe, der auch das Verzeichnis gehört.

Stellen Sie sich zum Beispiel vor, dass eine Gruppe von Mitarbeitern an Dateien im Verzeichnis `/usr/lib/emacs/site-lisp/` arbeitet. Einigen wird soweit vertraut, dass sie das Verzeichnis ändern dürfen, aber sicherlich nicht allen. Erstellen Sie zuerst eine `emacs` Gruppe mit folgendem Befehl:

```
/usr/sbin/groupadd emacs
```

Um den Verzeichnisinhalt mit der `emacs` Gruppe zu verknüpfen, geben Sie Folgendes ein:

```
chown -R root.emacs /usr/lib/emacs/site-lisp
```

Nun können Sie mit Hilfe von `gpasswd` die richtigen Benutzer zur Gruppe hinzufügen:

```
/usr/bin/gpasswd -a <username> emacs
```

Um den Benutzern tatsächlich zu gestatten, Dateien im Verzeichnis zu erstellen, verwenden Sie den folgenden Befehl:

```
chmod 775 /usr/lib/emacs/site-lisp
```

Wenn ein Benutzer eine neue Datei erstellt, wird diese der benutzereigenen Standardgruppe zugeordnet. Um dies zu verhindern, müssen Sie folgenden Befehl ausführen, der dafür sorgt, dass alle Dateien im Verzeichnis mit der Gruppe des Verzeichnis selbst (`emacs`) erstellt werden:

```
chmod 2775 /usr/lib/emacs/site-lisp
```

Zu diesem Zeitpunkt, da die Default-umask aller Benutzer 002 ist, können die Mitglieder der `emacs`-Gruppe Dateien im Verzeichnis `/usr/lib/emacs/site-lisp/` ändern, ohne dass der Administrator Rechte ändern müsste, jedesmal wenn eine neue Datei erzeugt wird.

6.5. Shadow-Utilities

In Mehrbenutzer-Umgebungen ist es sehr wichtig, *Shadow-Passwörter* zu verwenden, die im Rahmen des `shadow-utils` Paketes geliefert werden. Dies vergrößert die Sicherheit der System- Authentifizierungsdateien, weshalb das Installationsprogramm Shadow-Passwörter standardmäßig aktiviert.

Im Folgenden eine Auflistung der Vorteile, die Shadow-Passwörter im Vergleich zu der traditionellen Speichermethode von Passwörten auf UNIX-Systemen haben:

- Shadow-Passwörter erhöhen die Systemsicherheit dadurch, dass die verschlüsselten Passwörter (normalerweise in der Datei `/etc/passwd` abgelegt) im Verzeichnis `/etc/shadow` abgelegt werden, das nur von root gelesen werden kann.
- Liefern Informationen über das Altern von Passwörtern.
- Die Möglichkeit unter Verwendung der Datei `/etc/login.defs` die Sicherheitsbestimmungen besonders im Bezug auf veraltete Passwörter umzusetzen.

Die meisten Utilities, die mit dem `shadow-utils` Paket geliefert werden, arbeiten ordnungsgemäß, unabhängig davon, ob Shadow-Passwörter aktiviert sind oder nicht. Da allerdings Informationen über die Veralterung von Passwörtern ausschließlich in `/etc/shadow` gespeichert werden, funktionieren keine Befehle, die Informationen über die Veralterung von Passwörtern erzeugen oder verändern.

Below is a list of commands which do not work without first enabling shadow passwords:

- `chage`
- `gpasswd`
- `/usr/sbin/usermod -e` or `-f` options
- `/usr/sbin/useradd -e` or `-f` options

6.6. Zusätzliche Informationsquellen

Für weitere Informationen über Benutzer und Gruppen sowie über die Tools zu ihrer Verwaltung, siehe die folgenden Informationsquellen:

6.6.1. Installierte Dokumentation

- Man-Seiten zu diesen Themenbereichen — Es gibt eine Reihe von man-Seiten über die verschiedenen Anwendungen und Konfigurationsdateien, die beim Verwalten von Benutzern und Gruppen verwendet werden. Im Folgenden eine Liste der wichtigsten man-Seiten:

  Anwendungen zur Benutzer- und Gruppenverwaltung

  - `man chage` — Ein Befehl, der die Richtlinien zur Passwort-Veralterung und zum Verfall des Accounts verändert.
  - `gpasswd` — Ein Befehl zur Verwaltung der Datei `/etc/group`.
  - `man groupadd` — Ein Befehl, der Gruppen hinzufügt.
  - `man grpck` — Ein Befehl zur Überprüfung des der Datei `/etc/group`.
  - `man groupdel` — Ein Befehl zum Entfernen von Gruppen.
  - `man groupmod` — Ein Befehl zur Veränderung von Gruppen-Mitgliedschaften.
  - `man pwck` — Ein Befehl zur Überprüfung der `/etc/passwd` und der `/etc/shadow` Datei.
  - `man pwconv` — Ein Tool, das Standard-Passwörter in Shadow-Passwörter umwandelt.
  - `man pwunconv` — Ein Tool, das Shadow- Passwörter in Standard-Passwörter umwandelt.
  - `man useradd` — Ein Befehl, der Benutzer hinzufügt.
  - `man userdel` — Ein Befehl, der Benutzer entfernt.
  - `man usermod` — Ein Befehl, der Benutzer verändert.

  Konfigurationsdateien

  - `man 5 group` — Die Datei, die Gruppeninformation für das System enthält.
  - `man 5 passwd` — Die Datei, die Benutzerinformation für das System enthält.
  - `man 5 shadow` — Die Datei, die Passwörter und Informationen über den Verfall der Accounts enthält.

6.6.2. Bücher zum gleichen Thema

- *Red Hat Enterprise Linux Introduction to System Administration*; Red Hat, Inc. — Dieser Begleiter bietet einen Überblick über die Konzepte und Techniken der Systemverwaltung. Das Kapitel *Managing User Accounts and Resource Access* enthält großartige Informationen über die Verwaltung von Benutzer- und Gruppen- Accounts.

- *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Dieser Begleiter enthält weitere Informationen über die Verwaltung von Benutzern und Gruppen sowie über fortgeschrittene Konfigurationen von Genehmigungen mit ACLs. Für Details siehe die Kapitel *User and Group Configuration* und *Access Control Lists*.

- *Red Hat Enterprise Linux Sicherheitshandbuch*; Red Hat, Inc. — Dieser Begleiter informiert über Sicherheitsaspekte von Benutzer-Accounts, konkret über das Auswählen kompetenter Passwörter.

redhat

Kapitel 7.

Das X Window System

Während der Kernel das Herz von Red Hat Enterprise Linux darstellt, ist die vom *X Window System*, kurz *X* genannt, bereitgestellte grafische Umgebung für viele Benutzer das Gesicht des Betriebssystems.

In der UNIX™-Welt gibt es seit Jahrzehnten Umgebungen mit Fenstergestaltung, womit sie vielen der momentan gebräuchlichsten Betriebssystemen voraus war. Das X Window System ist nun die gebräuchlichste GUI für Unix-ähnliche Betriebssysteme.

Die graphische Umgebung von Red Hat Enterprise Linux wird von XFree86™ bereitgestellt, einem Open Source Softwareprojekt, an dem Hunderte von Entwicklern in der ganzen Welt arbeiten. XFree86 zeichnet sich durch eine schnelle Entwicklung, einen umfangreichen Support für verschiedene Hardware-Geräte und Architekturen sowie die Fähigkeit aus, unter verschiedenen Betriebssystemen und Plattformen zu laufen.

Das X Window System verwendet eine Client-Server-Architektur. Dabei wird ein *X-Server*-Prozess gestartet, mit dem sich *X-Client*-Prozesse über ein Netzwerk oder eine lokale Verbindung verknüpfen können. Der Serverprozess verwaltet die Kommunikation mit der Hardware wie zum Beispiel mit der Grafikkarte, dem Monitor, der Tastatur und der Maus. Der X-Client existiert im Benutzerbereich, und erstellt eine graphische Benutzerschnittstelle (*graphical user interface*, *GUI*) für den Benutzer, und gibt Anfragen an den X-Server weiter.

7.1. XFree86

Red Hat Enterprise Linux 3 verwendet XFree86 Version 4.x als Basis-X Window System, welches viele Cutting-Edge XFree86 Technologien beinhaltet. Dazu gehören 3D Hardwarebeschleunigung, XRender-Erweiterung für anti-aliased Fonts, ein modulares Treiber-basiertes Design und Unterstützung für moderne Video-Hardware und Eingabegeräte.

Wichtig

Red Hat Enterprise Linux stellt keine Serverpakete von XFree86 Version 3 mehr zur Verfügung. Ehe Sie auf die letzte Version von Red Hat Enterprise Linux aktualisieren, stellen Sie sicher, dass Ihre Grafikkarte mit der Version 4 von XFree86 kompatibel ist. Überprüfen Sie dies auf der Red Hat-HCL (Hardwarekompatibilitätsliste) unter dem URL http://hardware.redhat.com.

Das X Window System befindet sich hauptsächlich an zwei Speicherorten im Dateisystem:

/usr/X11R6/

Enthält X-Server, einige Client-Applikationen, bestimmten X-Headerdateien, Bibliotheken, Module und Dokumentation.

`/etc/X11/`

Enthält alle Konfigurationsdateien für die verschiedenen Komponenten des X Window Systems. Hierzu gehören Konfigurationsdateien für den X-Server, den älteren X-Font-Server (`xfs`), X-Display Manager und zahlreiche weitere grundlegende Komponenten.

Es ist wichtig zu beachten, dass die Konfigurationsdatei für die neuere Fontconfig-basierte Font-Architektur `/etc/fonts/fonts.conf` ist (was die Datei `/etc/X11/XftConfig` überflüssig

macht). Für weitere Informationen zur Konfiguration und zum Hinzufügen von Fonts, sehen Sie Abschnitt 7.4.

Da der XFree86-Server eine Reihe von fortgeschrittenen Tasks auf einer Vielzahl an Hardware durchführt, benötigt dieser eine detaillierte Konfiguration. Das Installationsprogramm installiert und automatisch konfiguriert XFree86, solange die XFree86 Pakete zur Installation ausgewählt sind. Wenn sich allerdings der Monitor oder die Grafikkarte ändert, muss XFree86 neu konfiguriert werden. Am besten verwenden Sie hierzu **X Configuration Tool** (`redhat-config-xfree86`).

Wenn Sie **X Configuration Tool** in einer aktiven X-Sitzung starten möchten, wechseln Sie zur **Schaltfläche des Hauptmenüs** (im Panel) => **Systemtools** => **Anzeigen**. Wenn Sie **X Configuration Tool** während einer X-Sitzung verwendet haben, müssen Sie sich von der aktuellen X-Sitzung abmelden und erneut anmelden, damit die Änderungen wirksam werden. Für weitere Informationen zur Verwendung von **X Configuration Tool** sehen Sie das Kapitel *Audio, Video und Multimedia* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

In einigen Fällen kann es notwendig sein die Konfigurationsdatei des XFree86 Server, `/etc/X11/XF86Config`, manuell zu bearbeiten. Für weitere Informationen zur Struktur dieser Datei sehen Sie Abschnitt 7.3.

7.2. Desktop-Umgebungen und Window Manager

Wenn der XFree86-Server erst einmal läuft, können X-Client-Applikationen zu diesem verbinden und eine GUI für den Benutzer erzeugen. Eine Anzahl von GUIs sind in Red Hat Enterprise Linux möglich, vom rudimentären *Tab Window Manager* zum hochentwickelten, interaktiven *GNOME* Desktop, mit welcher die meisten Red Hat Enterprise Linux Benutzer vertraut sind.

Um die letztere, weiter entwickelte GUI zu erzeugen, müssen zwei X-Client-Applikationen zum XFree86-Server verbinden: Eine *Desktop-Umgebung* und ein *Window Manager*.

7.2.1. Desktop-Umgebungen

Eine Desktop-Umgebung umfasst eine Anzahl verschiedenster X-Clients. Diese zusammengenommen stellen die graphische Benutzeroberfläche und Entwicklungsplattform dar.

Desktop-Umgebungen enthalten erweiterte Merkmale, die es X-Clients und anderen laufenden Prozessen ermöglichen, miteinander zu kommunizieren. Auf diese Weise können alle Applikationen, die für diese Umgebung geschrieben wurden, integriert und auf weitere Arten verwendet werden, wie beispielsweise die Drag-and-Drop Funktionen.

Red Hat Enterprise Linux liefert zwei Desktop-Umgebungen:

- *GNOME* — Die standardmäßige Desktop-Umgebung für Red Hat Enterprise Linux, welche auf dem GTK+ 2 graphischen Toolkit basiert.
- *KDE* — Eine weitere Desktop-Umgebung, welche auf dem Qt 3 graphischen Toolkit basiert.

Sowohl GNOME als auch KDE besitzen erweiterte Applikationen wie textverarbeitende Prozessoren, elektronische Kalkulationstabellen und Bedienerkonsolen-Geräte, mit denen Sie das Look and Feel vollständig steuern können. Beide Umgebungen können standardmäßige X-Clientanwendungen ausführen. Die meisten KDE-Anwendungen können auch in GNOME ausgeführt werden, wenn die Qt-Bibliotheken installiert sind.

7.2.2. Window Manager

Window Manager sind X-Clientprogramme, die die Art und Weise steuern, in der andere X-Clients positioniert, in ihrer Größe verändert oder bewegt werden. Window Manager liefern darüber hinaus

auch Titelleisten, Tastaturspezifizierung nach Tastatur oder Maus sowie benutzerspezifische Tasten- und Maustastenbindungen.

Fünf Window Manager sind in Red Hat Enterprise Linux enthalten:

- `kwin` — Der *KWin* Window Manager ist der Default bei der Auswahl der KDE Desktop-Umgebung. Dies ist ein effizienter Window Manager, der benutzerdefinierte Themen unterstützt.
- `metacity` — Der *Metacity* Window Manager ist der Default bei der Auswahl der GNOME Desktop-Umgebung. Es ist ein einfacher und effizienter Window Manager, der benutzerdefinierte Themen unterstützt.
- `mwm` — Der *Motif* Window Manager ist ein Standalone Window Manager, mit grundlegenden Funktionen. Da dieser als Standalone entwickelt wurde, sollte er weder mit der GNOME noch mit der KDE Desktop-Umgebung ausgeführt werden.
- `twm` — Ein minimalistischer *Tab Window Manager*, der im Vergleich am wenigsten Funktionalität bietet. Er kann als Standalone, oder zusammen mit einer Desktop-Umgebung ausgeführt werden und wird als Teil von XFree86 installiert.

Diese Window Manager können als einzelne X-Clients ausgeführt werden, womit auch die Unterschiede deutlicher werden. Geben Sie den Befehl `xinit <Pfad-zum-Window-Manager>` ein, wobei `<Pfad-zum-Window-Manager>` der Speicherort der Binärdatei des Window Managers ist. Die Binärdatei kann ermittelt werden, indem Sie `which <Window-Manager-Name>` eingeben, wobei `<Window-Manager-Name>` der Name des gesuchten Window Manager ist.

7.3. XFree86-Server-Konfigurationsdateien

Der XFree86 Server ist eine einzelne ausführbare Binärdatei (`/usr/X11R6/bin/XFree86`), welche alle benötigten X Server Module zur Laufzeit vom Verzeichnis `/usr/X11R6/lib/modules/` lädt. Einige dieser Module werden automatisch geladen, während andere in der Konfigurationsdatei von XFree86 Server angegeben werden müssen.

Die XFree86 Server und damit zusammenhängende Konfigurationsdateien sind im Verzeichnis `/etc/X11/` abgelegt. Die Konfigurationsdatei für XFree86 Server ist `/etc/X11/XF86Config`. Wenn Red Hat Enterprise Linux installiert ist, werden die Konfigurationsdateien für XFree86 mithilfe der während der Installation gesammelten Informationen erstellt.

7.3.1. `XF86Config`

Auch wenn Sie `/etc/X11/XF86Config` kaum manuell bearbeiten müssen, ist es sinnvoll, deren einzelnen Bereiche und optionalen Parameter zu kennen. Dies ist vor allem während der Fehlersuche vorteilhaft.

7.3.1.1. Die Struktur

Die Datei `/etc/X11/XF86Config` besteht aus zahlreichen Abschnitten, welche einen jeweils spezifischen Teil der System-Hardware ansprechen.

Jeder Abschnitt beginnt mit einer `Section "<Sektionsname>"`- Zeile und endet mit einer `EndSection`-Zeile. Innerhalb jedes einzelnen Abschnitts befinden sich verschiedene Zeilen mit einem Optionsnamen und mindestens einem Optionswert, der auch in Anführungszeichen (`"`) angegeben sein kann.

Mit einem Hash-Symbol [#] beginnende Zeilen werden vom XFree86-Server nicht gelesen und stellen Kommentare für den Benutzer dar.

Einige der Optionen in `/etc/X11/XF86Config` akzeptieren boolesche Werte, was die gegebene Funktion entweder ein oder aus schaltet. Verwendbare boolesche Werte sind:

- `1`, `on`, `true`, oder `yes` — Schaltet die Option ein.
- `0`, `off`, `false`, oder `no` — Schaltet die Option aus.

Folgend sind einige der wichtigeren Abschnitte aufgelistet, wie diese in einer typischen `/etc/X11/XF86Config` Datei vorkommen. Genauere Informationen zur Konfigurationsdatei des XFree86 Server können in den man-Seiten zu `XF86Config` gefunden werden.

7.3.1.2. `ServerFlags`

Der optionale Abschnitt `ServerFlags` enthält verschiedene allgemeine XFree86 Server-Einstellungen. Diese Einstellungen können mit Optionen des Abschnitts `ServerLayout` überschrieben werden (sehen Sie Abschnitt 7.3.1.3 für genaueres).

Jeder Eintrag im Abschnitt `ServerFlags` ist jeweils in einer eigenen Zeile, die mit dem Term `Option` beginnt und von einer in doppelte Anführungszeichen (`"`) eingeschlossenen Option gefolgt wird.

Folgend ist ein Beispiel eines `ServerFlags`-Abschnitts:

```
Section "ServerFlags"
      Option "DontZap" "true"
EndSection
```

Folgend ist eine Liste der nützlichsten Optionen:

- `"DontZap" "<`*`boolean`*`>"` — Wenn der Wert von <*boolean*> auf true gesetzt ist, verhindert dies, dass die Tastenkombination [Strg]-[Alt]-[Rücktaste] verwendet wird, die den XFree86-Server sofort beendet.
- `"DontZoom" "<`*`boolean`*`>"` — Wenn der Wert von <*boolean*> true ist, verhindert, dass die Tastenkombinationen [Strg]-[Alt]-[Zehnertastatur-Plus] und [Strg]-[Alt]-[Zehnertastatur-Minus] verwendet werden, um sich durch konfigurierte Grafikauflösungen zu bewegen.

7.3.1.3. `ServerLayout`

Der Abschnitt `ServerLayout` bindet Eingabe- und Ausgabegeräte, die vom XFree86 Server kontrolliert werden. Dieser Abschnitt muss zumindest ein Ausgabegerät und zwei Eingabegeräte (Tastatur und Maus) angeben.

Das folgende Beispiel zeigt einen typischen `ServerLayout`-Abschnitt:

```
Section  "ServerLayout"
        Identifier     "Default Layout"
        Screen      0  "Screen0" 0 0
        InputDevice    "Mouse0" "CorePointer"
        InputDevice    "Keyboard0" "CoreKeyboard"
EndSection
```

Die folgenden Einträge sind die in einem `ServerLayout`-Abschnitt am häufigsten verwendeten:

- `Identifier` — Ein eindeutiger Name, der für die Beschreibung dieses `ServerLayout`-Abschnitts verwendet wird.
- `Screen` — Der Name eines `Screen`-Abschnitts, der mit dem XFree86 Server verwendet wird. Es können mehr als eine `Screen`-Option vorkommen.

Folgend ist ein Beispiel eines typischen `Screen`-Eintrags:

```
Screen      0  "Screen0" 0 0
```

Die erste Zahl in diesem Beispiel eines `Screen`-Eintrags (`0`) gibt an, dass der erste *Anschluss* auf der Grafikkarte die im `Screen`-Abschnitt angegebene Konfiguration mit dem Identifier `"Screen0"` verwendet.

Sollte die Grafikkarte mehr als einen Anschluss haben, sind weitere `Screen`-Einträge mit unterschiedlichen Nummern und Identifiern für `Screen`-Abschnitte von Nöten.

Die Nummern auf der rechten Seite liefern die X- und Y-Koordinaten für die linke obere Ecke des Bildschirms (standardmäßig `0 0`).

- `InputDevice` — Gibt den Namen eines `InputDevice`-Abschnitts an, der mit dem XFree86 Server verwendet wird.

  Es muss zumindest zwei `InputDevice`-Einträge geben: Einer für die Standardmaus und einer für die Standardtastatur. Die Optionen `CorePointer` und `CoreKeyboard` weisen darauf hin, dass es sich um primäre Maus und Tastatur handelt.

- `Option "<option-name>"` — Ein optionaler Eintrag, der weitere Parameter für diesen Abschnitt angibt. Jede der hier aufgeführten Optionen überschreibt die Optionen im Abschnitt `ServerFlags`.

  Ersetzen Sie *<option-name>* hier mit einer der in den XF86Config man-Seiten aufgelisteten Optionen.

Es ist möglich mehr als einen `ServerLayout`-Abschnitt anzugeben. Der Server wird jedoch nur den ersten einlesen, außer, es wird eine anderer `ServerLayout`-Abschnitt als Befehlszeilenargument angegeben.

7.3.1.4. `Files`

Der `Files`-Abschnitt legt für XFree86 Server wichtige Pfade wie zum Beispiel den Fontpfad fest.

Das folgende Beispiel zeigt einen typischen `Files`-Abschnitt:

```
Section "Files"
        RgbPath      "/usr/X11R6/lib/X11/rgb"
        FontPath     "unix/:7100"
EndSection
```

Folgende Einträge sind die in einem `Files`-Abschnitt am häufigsten verwendeten:

- `RgbPath` — Gibt den Speicherort der RGB Farbdatenbank an. Diese Datenbank definiert alle in XFree86 gültigen Farbnamen und bindet diese deren entsprechenden RGB-Werten.
- `FontPath` — Gibt an, wo der XFree86 Server verbinden muss, um Fonts vom `xfs` Font-Server zu erhalten.

  Standardmäßig ist `FontPath unix/:7100`. Auf diese Weise wird der XFree86 Server angewiesen, Font-Informationen mithilfe von UNIX-Domänen-Sockets für die Kommunikation zwischen den Prozessen (IPC) abzurufen.

  In Abschnitt 7.4 finden Sie weitere Informationen über XFree86 und Fonts.

- `ModulePath` — Ermöglicht Ihnen (optional) die Einstellung von mehreren Verzeichnissen, die für die Speicherung von XFree86 Server Modulen verwendet werden.

7.3.1.5. `Module`

Der Abschnitt `Module` gibt dem XFree86 Server an, welche Module des `/usr/X11R6/lib/modules`-Verzeichnisses zu laden sind. Die Module statten den XFree86 Server mit zusätzlichen Funktionen aus.

Folgend ist ein Beispiel eines typischen `Module`-Abschnitts:

```
Section "Module"
 Load  "dbe"
 Load  "extmod"
 Load  "fbdevhw"
 Load  "glx"
 Load  "record"
 Load  "freetype"
 Load  "typel"
 Load  "dri"
EndSection
```

7.3.1.6. `InputDevice`

Jeder `InputDevice`-Abschnitt konfiguriert ein Input-Gerät wie eine Maus oder eine Tastatur, das für die Eingabe von Informationen in das System mithilfe des XFree86 Servers verwendet wird. Die meisten Systeme besitzen mindestens zwei `InputDevice`-Abschnitte, Tastatur und Maus.

Das folgende Beispiel zeigt einen typischen `InputDevice`-Abschnitt für eine Maus:

```
Section "InputDevice"
 Identifier  "Mouse0"
 Driver      "mouse"
 Option     "Protocol" "IMPS/2"
 Option     "Device" "/dev/input/mice"
 Option     "Emulate3Buttons" "no"
EndSection
```

Die folgenden Einträge werden am häufigsten in einem `InputDevice`-Abschnitt verwendet:

- `Identifier` — Gibt einen eindeutigen Namen für diesen `InputDevice`-Abschnitt an. Dieser Eintrag ist notwendig.
- `Driver` — Gibt XFree86 den Namen des Treibers an, der für die Verwendung des Geräts zu laden ist.
- `Option` — Gibt Geräte-bezogene Optionen an.

  Für eine Maus, enthalten diese Optionen Folgende:

  - `Protokoll` — Gibt das von der Maus verwendete Protokoll an, wie `IMPS/2`.
  - `Device` — Gibt den Ort des physischen Geräts an.
  - `Emulate3Buttons` — Gibt an, ob eine Zwei-Tasten-Maus eine dritte Taste, wenn beide Tasten gleichzeitig gedrückt werden, emulieren soll.

  Sehen Sie die XF86Config man-Seiten für eine Liste der gültigen Optionen.

Der Abschnitt `InputDevice` enthält einige Kommentare, die dem Benuzter das Konfigurieren weiterer Optionen ermöglicht.

7.3.1.7. `Monitor` Abschnitt

Jeder `Monitor`-Abschnitt konfiguriert einen Typ von Monitor, der vom System verwendet wird. Mindestens ein `Monitor`-Abschnitt muss vorhanden sein, zusätzliche können bestehen, einen für jeden vom Rechner verwendeten Typ von Monitor.

Der beste Weg, einen Monitor einzurichten, ist beim Konfigurieren von X während des Installationsprozesses oder durch Verwendung von **X Configuration Tool**. Für weiteres zur Verwendung von **X Configuration Tool**, sehen Sie da Kapitel *X Window System-Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Das folgende Beispiel zeigt einen typischen `Monitor`-Abschnitt:

```
Section "Monitor"
 Identifier   "Monitor0"
 VendorName   "Monitor Vendor"
 ModelName    "DDC Probed Monitor - ViewSonic G773-2"
 DisplaySize  320 240
 HorizSync    30.0 - 70.0
 VertRefresh  50.0 - 180.0
EndSection
```

Warnung

Seien Sie vorsichtig, wenn Sie die Werte im `Monitor`-Abschnitt der Datei `/etc/X11/XF86Config` manuell bearbeiten. Falsche Werte in diesem Abschnitt können Ihren Monitor beschädigen. Schlagen Sie in der Dokumentation Ihres Monitors die verfügbaren sicheren Parameter nach.

Folgend sind häufig im `Monitor`-Abschnitt verwendete Einträge:

- `Identifier` — Verleiht dem Monitor einen eindeutigen Namen. Dieser Eintrag ist erforderlich.
- `VendorName` — Ein optionaler Eintrag, welcher den Hersteller des Monitors angibt.
- `ModelName` — Ein optionaler Eintrag, welcher den Namen des Models des Monitors angibt.
- `DisplaySize` — Ein optionaler Eintrag, welcher, in Millimetern, die physische Größe des Bildschirmbereichs angibt.
- `HorizSync` — Gibt XFree86 die Bandbreite der Horizontalfrequenz in kHz an, die mit dem Monitor kompatibel ist. Diese Werte werden vom XFree86 Server als Richtlinie verwendet, so dass dieser weiß, ob bestimmte Werte eines `Modeline`-Eintrags für den Monitor zu verwenden sind.
- `VertRefresh` — Listet die vom Monitor unterstützten vertikalen Bildwiederholfrequenzen in kHz auf. Diese Werte werden vom XFree86 Server als Richtlinie verwendet, so dass dieser weiß, ob bestimmte Werte eines `Modeline`-Eintrags für den Monitor zu verwenden sind.
- `Modeline` — Dient der optionalen Angabe der Grafikmodi des Monitors bei besonderen Auflösungen mit bestimmten Horizontal- und Vertikalfrequenzen. Sehen Sie die man-Seiten zu `XF86Config` für eine genauere Beschreibung der `Modeline`-Einträge.
- `Option "<option-name>"` — Ein optionaler Eintrag, der weitere Parameter für diesen Abschnitt angibt. Ersetzen Sie *<option-name>* mit einer gültigen, in den man-Seiten zu XF86Config aufgelisteten Option.

7.3.1.8. `Device`

Jeder `Device`-Abschnitt konfiguriert eine Grafikkarte für das System. Ein `Device`-Abschnitt muss vorhanden sein. Weitere können bestehen, einer für jede auf dem Rechner installierte Grafikkarte.

Der beste Weg eine Grafikkarte einzurichten, ist beim Konfigurieren von X während des Installationsprozesses oder durch Verwendung von **X Configuration Tool**. Für weiteres zur Verwendung von **X Configuration Tool**, sehen Sie da Kapitel *X Window System-Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Das folgende Beispiel zeigt einen typischen `Device`-Abschnitt für eine Grafikkarte:

```
Section "Device"
 Identifier  "Videocard0"
 Driver      "mga"
 VendorName  "Videocard vendor"
 BoardName   "Matrox Millennium G200"
 VideoRam    8192
        Option      "dpms"
EndSection
```

Die folgenden Einträge sind häufig in einem `Device`-Abschnitt verwendet:

- `Identifier` — Ein eindeutiger Name für diesen `Device`-Abschnitt. Dies ist ein notwendiger Eintrag.
- `Driver` — Gibt an, welchen Treiber der XFree86 Server laden muss, um die Grafikkarte verwenden zu können. Eine Liste von Treibern kann in der Datei `/usr/X11R6/lib/X11/Cards` gefunden werden, welche mit dem Paket `hwdata` installiert wird.
- `VendorName` — Gibt (optional) den Hersteller der Grafikkarte an.
- `BoardName` — Gibt (optional) den Namen der Grafikkarte an.
- `VideoRam` — Der RAM-Speicher (optional) der Grafikkarte in Kilobytes. Diese Einstellung ist normalerweise nicht notwendig, da der XFree86-Server gewöhnlich die Grafikkarte automatisch auf den verfügbaren Speicher prüft. Es gibt jedoch Grafikkarten, die XFree86 nicht automatisch erkennen kann, weswegen Ihnen diese Option die Möglichkeit bietet, manuell den Grafik-RAM anzugeben.
- `BusID` — Gibt (optional) den Bus an, in dem sich die Grafikkarte befindet. Diese Option ist nur bei Systemen mit mehreren Karten notwendig.
- `Screen` — Ein optionaler Eintrag, der angibt, welchen Anschluss der Grafikkarte dieser `Device`-Abschnitt konfiguriert. Diese Option ist nur bei Grafikkarten mit mehr als einem Anschluss nützlich.

  Wenn mehrere Monitore an eine Grafikkarte angeschlossen sind, dann müssen auch verschiedene `Device`-Abschnitte mit einem jeweils unterschiedlichen `Screen`-Wert zur Verfügung stehen.

  Der Wert eines `Screen`-Eintrags ist eine ganzzahlige Nummer. Der erste Anschluss hat den Wert `0` und für jeden weiteren Anschluss wird diese Zahl um eins erhöht.
- `Option "<option-name>"` — Ein optionaler Eintrag, der weitere Parameter für diesen Abschnitt angibt. Ersetzen Sie *<option-name>* mit einer gültigen, in den man-Seiten zu XF86Config aufgelisteten Option.

  Eine der häufiger verwendeten Optionen ist `"dpms"`, welches die Service Star Energy Compliance für den Monitor einschaltet.

7.3.1.9. `Screen`

Jeder `Screen`-Abschnitt bindet eine Grafikkarte (oder einen Anschluss auf einer Grafikkarte) an einen Monitor, indem dieser den `Device`-Abschnitt und den jeweiligen `Monitor`-Abschnitt für jeden der Anschlüsse referenziert. Ein `Screen`-Abschnitt muss vorhanden sein, weitere bestehen für jede zusätzliche Kombination von Grafikkarte (oder Anschluss) zu Monitor auf dem gegebenen Rechner.

Folgend ist ein Beispiel eines typischen `Screen`-Abschnitts:

```
Section "Screen"
 Identifier "Screen0"
 Device     "Videocard0"
 Monitor    "Monitor0"
 DefaultDepth     16
 SubSection "Display"
  Depth     24
  Modes    "1280x1024" "1280x960" "1152x864" "1024x768" "800x600" "640x480"
 EndSubSection
 SubSection "Display"
  Depth     16
  Modes    "1152x864" "1024x768" "800x600" "640x480"
 EndSubSection
EndSection
```

Folgende Einträge sind häufig in einem `Screen`-Abschnitt verwendet:

- `Identifier` — Ein eindeutiger Name für diesen `Screen`-Abschnitt. Dies ist ein notwendiger Eintrag.
- `Device` — Gibt einen eindeutigen Namen eines `Device`-Abschnitts an. Dieser Eintrag ist erforderlich.
- `Monitor` — Gibt einen eindeutigen Namen eines `Monitor`-Abschnitts an. Dieser Eintrag ist notwendig.
- `DefaultDepth` — Gibt die Farbtiefe in Bits an. Im vorangegangenen Beispiel ist `16`, was mehrere tausende von Farben ermöglicht, der Default-Wert. Mehrere `DefaultDepth`-Einträge sind zulässig, aber einer muss mindestens vorhanden sein.
- `SubSection "Display"` — Gibt die Bildschirmmodi an, die bei einer spezifischen Farbtiefe zur Verfügung stehen. Ein `Screen`-Abschnitt kann mehrere `Display`-Unterabschnitte haben, es muss allerdings zumindest einer für die in `DefaultDepth` angegebene Farbtiefe bestehen.
- `Option "<option-name>"` — Ein optionaler Eintrag, der weitere Parameter für diesen Abschnitt angibt. Ersetzen Sie *<option-name>* mit einer gültigen, in den man-Seiten zu XF86Config aufgelisteten Option.

7.3.1.10. `DRI`

Beim optionalen `DRI`-Abschnitt *Direct Rendering Infrastructure* (*DRI*) handelt es sich um eine Schnittstelle, die es 3D-Software-Applikationen ermöglicht, die 3D-Hardwarebeschleunigung moderner und unterstützter Grafikhardware zu nutzen. Darüber hinaus verbessert DRI die Leistung der 2D-Hardwarebeschleunigung, sofern vom Treiber unterstützt.

Dieser Abschnitt wird ignoriert, es sei denn, DRI wird im `Module`-Abschnitt aktiviert.

Das folgende Beispiel zeigt einen typischen `DRI`-Abschnitt:

```
Section "DRI"
        Group        0
        Mode         0666
EndSection
```

Unterschiedliche Grafikkarten verwenden DRI auf unterschiedliche Weise. Bevor Sie DRI-Werte ändern, lesen Sie bitte zuerst die Datei `/usr/X11R6/lib/X11/doc/README.DRI`.

7.4. Fonts

Red Hat Enterprise Linux verwendet zwei Methoden, um Fonts und die Anzeige unter XFree86 zu regeln. Das neuere Fontconfig Font-Subsystem vereinfacht das Font-Management und liefert erweitere Anzeigefunktionen, wie Anti-Aliasing. Dieses System wird automatisch für Applikationen verwendet, welche unter Verwendung entweder des Qt 3 oder des GTK+ 2 graphischen Toolkits entwickelt wurden.

Aus Gründen der Kompatibilität, enthält Red Hat Enterprise Linux auch das originale, Core X, Font-Subsystem. Dieses System, welches mehr als 15 Jahre alt ist, ist um den *X Font Server* (*xfs*) basiert.

Dieser Abschnitt beschreibt das Konfigurieren von Fonts unter Verwendung beider Systeme.

7.4.1. Fontconfig

Das Fontconfig Font-Subsystem erlaubt Applikationen den Zugriff auf Fonts des Systems und die Verwendung von Xft oder eines anderen Render-Mechanismus, um Fontconfig Fonts mit einem fortgeschrittenen Anti-Aliasing zu versehen. Graphische Applikationen können die Xft-Library mit Fontconfig dazu benutzen, Text auf dem Bildschirm darzustellen.

Mit der Zeit wird das Fontconfig/Xft Font-Subsystem das Core X Font-Subsystem vollständig ablösen.

Wichtig

Das Fontconfig Font-Subsystem arbeitet noch nicht mit **OpenOffice.org**, das eigene Font-Render-Technologien verwendet.

Es ist wichtig zu beachten, dass Fontconfig die Konfigurationsdatei `/etc/fonts/fonts.conf` teilt, was das alte `/etc/X11/XftConfig` ersetzt. Die Fontconfig Konfigurationsdatei sollte nicht manuell bearbeitet werden.

Tipp

Während dem Übergang zum neuen Font-System, werden GTK+ 1.2 Applikationen von Änderungen, welche über den **Font Preferences** Dialog (**Main Menu Button** [auf dem Panel] => **Preferences** => **Font**) getätigt werden, nicht betroffen. Für diese Applikationen kann eine Font durch Hinzufügen der folgenden Zeile zur Datei `~/.gtkrc.mine` konfiguriert werden:

```
style "user-font" {

fontset = "<font-specification>"

}

widget_class "*" style "user-font"
```

Ersetzen Sie *<font-specification>* mit einer Fontangabe im traditionellen, von X-Applikationen verwendeten, Format, wie `-adobe-helvetica-medium-r-normal--*-120-*-*-*-*-*-*`. Eine vollständige Liste der Core-Fonts kann durch Ausführen von `xlsfonts` erhalten oder durch Verwendung von `xfontsel` interaktiv erzeugt werden.

7.4.1.1. Hinzufügen von Fonts zu Fontconfig

Das Hinzufügen von neuen Fonts zum Fontconfig-Subsystem ist ein einfacher und direkter Vorgang.

1. Um Fonts systemweit hinzuzufügen, kopieren Sie die neuen Fonts in das Verzeichnis `/usr/share/fonts/local/`.

   Um Fonts für einen gewissen Benutzer hinzuzufügen, kopieren Sie die Fonts in das Unterverzeichnis `.fonts/` im Hauptverzeichnis des Benutzers.

2. Benutzen Sie den Befehl `fc-cache` um die Font-Information im Cache zu aktualisieren, wie Folgend beschrieben:

   ```
   4fc-cache <path-to-font-directory>
   ```

   Ersetzen Sie *<path-to-font-directory>* mit dem Verzeichnis, das die neuen Fonts enthält (entweder `/usr/share/fonts/local/` oder `/home/<user>/.fonts/`).

Tipp

Individuelle Benutzer können Fonts auch graphisch installieren, indem Sie `fonts:///` in der Adress-Leiste von **Nautilus** angeben, und neue Font-Dateien über Drag-and-Drop dort hinein kopieren.

Wichtig

Wenn der Font-Dateiname in `.gz` ended, ist dies eine komprimierte Datei und diese kann nicht direkt verwendet werden. Die darin enthaltenen Dateien müssen zuerst extrahiert werden. Verwenden Sie dazu den Befehl `gunzip` oder doppel-klicken Sie die Datei und kopieren Sie die Font mittels Drag-and-Drop in ein Verzeichnis in **Nautilus**.

7.4.2. Core X Font-System

Aus Gründen der Kompatibilität, stellt Red Hat Enterprise Linux das Core X Font-Subsystem, das den X Font Server (`xfs`) verwendet, auch weiterhin zur Verfügung, um den X-Client-Applikationen Fonts bereitzustellen.

Der XFree86 Server sucht nach den im `FontPath`-Eintrag des `Files`-Abschnitt der Konfigurationsdatei `/etc/X11/XF86Config` angegebenen Fonts. Sehen Sie Abschnitt 7.3.1.4 für weitere Information zum `FontPath`-Eintrag.

Der XFree86-Server verbindet zum `xfs`-Server auf einem angegebenen Port, um Font-Informationen zu erfragen. Aus diesem Grund muss der `xfs`-Service laufen, damit X starten kann. Für weitere Informationen zum Konfigurieren von Services für einen bestimmten Runlevel, sehen Sie das Kapitel *Zugriffskontrolle von Services* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

7.4.2.1. `xfs`-Konfiguration

Das `/etc/rc.d/init.d/xfs`-Skript startet den `xfs`-Server. In der Datei `/etc/X11/fs/config` können verschiedene Optionen konfiguriert werden.

Die Folgende ist eine Liste der häufiger verwendeten Optionen:

- `alternate-servers` — Gibt eine Liste alternativer Font-Server an, die verwendet werden können, wenn dieser Server nicht verfügbar ist. Die einzelnen Font-Server sind durch Kommas zu trennen.
- `catalogue` — Eine geordnete Liste mit zu verwendenden Font-Pfaden. Font-Pfade müssen dabei durch Kommas getrennt werden.

  Sie können die Zeichenkette `:unscaled` unmittelbar nach dem Font-Pfad verwenden, um die nicht nicht skalierten Fonts dieses Pfades zuerst zu laden. Anschließend können Sie den gesamten Pfad erneut angeben, um andere skalierte Fonts zu laden.
- `client-limit` — Stellt die maximale Anzahl an Clients ein, die von diesem Font-Server bedient werden können. Der Standardwert ist `10`.
- `clone-self` — Gibt an, ob der Font-Server eine neue Version von sich selbst klont, wenn `client-limit` erreicht ist. Standardmäßig ist diese Option auf `on` eingestellt.
- `default-point-size` — Stellt die standardmäßige Punktgröße für alle Fonts ein, die keinen spezifischen Wert aufweisen. Der Standardwert von `120` entspricht 12-Punkt-Fonts.
- `default-resolutions` — Gibt eine Liste mit vom XFree86-Server unterstützten Auflösungen an. Die Auflösungen der Liste müssen dabei durch Kommas getrennt sein.
- `deferglyphs` — Gibt an, ob mit dem Laden von *glyphs* (der Grafik, die eine Font visuell darstellt) gewartet werden soll. Diese Option kann mit `none` deaktiviert werden. Alternativ kann sie auch für alle Fonts, `all`, oder nur für 16-Bit-Fonts, `16`, aktiviert werden.
- `error-file` — Hiermit können Sie den Pfad- und Dateinamen von Speicherorten eingeben, wo `xfs`-Fehler protokolliert werden können.
- `no-listen` — Weist `xfs` an, bestimmte Protokolle nicht abzuhören. Standardmäßig ist diese Option auf `tcp` eingestellt, um zu verhindern, dass `xfs` TCP-Ports abhört. Dies geschieht aus Sicherheitsgründen.

Tipp

Wenn `xfs` verwendet wird, um Fonts über das Netzwerk bereit zu stellen, entfernen Sie diese Zeile.

- `port` — Gibt den TCP-Port an, den `xfs` abhört, wenn `no-listen` entweder nicht vorhanden ist oder auskommentiert wurde.
- `use-syslog` — Gibt an, ob das System-Error-Log verwendet werden soll.

7.4.2.2. Hinzufügen von Fonts zu `xfs`

Um dem Core X Font-Subsystem (`xfs`) Fonts hinzuzufügen, folgen Sie diesen Schritten:

1. Erstellen Sie ein Font-Verzeichnis, sofern nicht vorhanden, mit dem Namen `/usr/share/fonts/local/` unter Verwendung des folgenden Befehls als root:
   ```
   mkdir /usr/share/fonts/local/
   ```
   Sollte es nötig sein, das Verzeichnis `/usr/share/fonts/local/` zu erstellen, muss dieses zum `xfs`-Pfad hinzugefügt werden. Dies geschieht durch Aufrufen des folgenden Befehls als root:
   ```
   chkfontpath --add /usr/share/fonts/local/
   ```
2. Kopieren Sie die neuen Font-Dateien in das Verzeichnis `/usr/share/fonts/local/`.
3. Aktualisieren Sie die Font-Information durch Ausführen des folgenden Befehls als root:
   ```
   ttmkfdir -d /usr/share/fonts/local/ -o /usr/share/fonts/local/fonts.scale
   ```

4. Laden Sie die Font-Server Konfigurationsdatei von `xfs` neu, indem Sie folgenden Befehl als root eingeben:
   ```
   service xfs reload
   ```

7.5. Runlevels und XFree86

In den meisten Fällen konfiguriert eine Standardinstallation von Red Hat Enterprise Linux einen Rechner zum Booten in die graphische Oberfläche, als Runlevel 5 bekannt. Es ist allerdings möglich, in eine text-basierte Oberfläche, auch Runlevel 3 genannt, zu Booten und eine X-Session von dort zu beginnen.

Für mehr Informationen zu Runlevels, sehen Sie Abschnitt 1.4.

Dieser Abschnitt behandelt das Starten von XFree86 in beide, Runlevel 3 und Runlevel 5.

7.5.1. Runlevel 3

Wenn Sie sich im Runlevel 3 befinden, ist es empfehlenswert X mit dem Befehl `startx` zu starten. `startx` ist ein Front-End zum Befehl `xinit`, das den XFree86-Server startet und ihn mit X-Clients verbindet. Da Sie bereits im Runlevel 3 im System angemeldet sein müssen, startet `startx` weder den Display-Manager, noch authentifiziert er Benutzer. Sehen Sie Abschnitt 7.5.2 für weitere Informationen zu Display-Managern.

Wenn `startx` startet, wird nach der Datei `.xinitrc` im Home-Verzeichnis des Benutzers gesucht, um die Desktop-Umgebung und eventuell andere auszuführenden X-Clients zu bestimmen. Ist diese Datei nicht vorhanden, wird das Standardskript `/etc/X11/xinit/xinitrc` ausgeführt.

Das standardmäßige `xinitrc`-Skript sucht anschließend im Home-Verzeichnis des Benutzers nach benutzerdefinierten Dateien und standardmäßigen Systemdateien, einschließlich `.Xresources`, `.Xmodmap` und `.Xkbmap`, und nach `Xresources`, `Xmodmap` und `Xkbmap` im Verzeichnis `/etc/X11/`. Die Dateien `Xmodmap` und `Xkbmap` werden, sofern sie vorhanden sind, vom Dienstprogramm `xmodmap` verwendet, um die Tastatur zu konfigurieren. Die `Xresources`-Dateien werden gelesen, um bestimmten Applikationen spezifische Präferenzwerte zuzuweisen.

Nachdem diese Optionen eingestellt sind, führt das Skript `xinitrc` alle Skripte im Verzeichnis `/etc/X11/xinit/xinitrc.d` aus. Ein wichtiges Skript dieses Verzeichnisses ist `xinput`, womit Einstellungen wie die zu verwendende Standardsprache und Desktop-Umgebung konfiguriert werden.

Anschließend versucht das Skript `xinitrc`, `.Xclients` im Home-Verzeichnis des Benutzers auszuführen, und kehrt zu `/etc/X11/xinit/Xclients` zurück, wenn diese Datei nicht gefunden wird. Der Zweck der Datei `Xclients` ist der Start der Desktop-Umgebung oder, wenn möglich, nur eines einfachen Window Managers. Das Skript `.Xclients` des Home-Verzeichnisses startet die vom Benutzer angegebene Desktop-Umgebung oder den Window Manager in der Datei `.Xclients-default`. Wenn `.Xclients` nicht im Home-Verzeichnis vorhanden ist, versucht das Standardskript `/etc/X11/init/Xclients`, eine andere Desktop-Umgebung zu starten und verwendet hierzu zunächst GNOME, dann KDE und anschließend `twm`.

Wenn der Benutzer sich aus X abmeldet, wird dieser sich wieder im Textmodus des Runlevel 3 befinden.

7.5.2. Runlevel 5

Wenn das System in den Runlevel 5 bootet, wird eine spezielle X-Client-Applikation, Display-Manager genannt, gestartet. Ein Benutzer muss sich gegen den Display-Manager authentifizieren, bevor Desktop-Umgebungen oder Window-Manager gestartet werden.

Je nach den auf Ihrem System installierten Desktop-Umgebungen stehen drei verschiedene Display Manager für die Benutzer-Authentifizierung zur Verfügung.

- `gdm` — Der in Red Hat Enterprise Linux standardmäßig ausgewählte Display-Manager. `gdm` erlaubt dem Benutzer Spracheinstellungen zu ändern, den Computer herunterzufahren, neu zu starten oder sich im System anzumelden.
- `kdm` — Der KDE Display Manager erlaubt dem Benutzer, den Computer herunterzufahren, neu zu starten oder sich im System anzumelden.
- `xdm` — Ein sehr einfacher Display Manager, welcher es dem Benutzer lediglich erlaubt sich im System anzumelden.

Wenn das System in Runlevel 5 bootet, bestimmt das Skript `prefdm` den bevorzugten Display-Manager für die Benutzer-Authentifizierung. Hierzu wird die Datei `/etc/sysconfig/desktop` verwendet. Sehen Sie die Datei `/usr/share/doc/initscripts-<version-number>/sysconfig.txt` (wobei *<version-number>* die Versionsnummer des `initscripts`-Pakets ist) für eine Liste der für diese Datei verfügbaren Optionen.

Jeder Display Manager verwendet die Datei `/etc/X11/xdm/Xsetup_0`, um den Anmeldebildschirm einzurichten. Sobald sich der Benutzer am System anmeldet, wird das Skript `/etc/X11/xdm/GiveConsole` ausgeführt, um dem Benutzer die Konsole als Eigentum zuzuweisen. Dann wird das Skript `/etc/X11/xdm/Xsession` ausgeführt, um viele der Aufgaben auszuführen, die in der Regel vom Skript `xinitrc` beim Start von X in Runlevel 3 ausgeführt werden. Dazu gehören u.a. das Festlegen der System- und Benutzerressourcen oder das Ausführen der Skripte im Verzeichnis `/etc/X11/xinit/xinitrc.d/`.

Der Benutzer kann mithilfe des `gdm` oder `kdm` Display-Managers angeben, welche Desktop-Umgebung bei der Authentifizierung verwendet werden sollen. Die Display-Manager können im Menü **Sitzung** ausgewählt werden. Ist die Desktop-Umgebung nicht im Display-Manager angegeben, prüft das Skript `/etc/X11/xdm/Xsession` die Dateien `.xsession` und `.Xclients` im Home-Verzeichnis, um zu entscheiden, welche Desktop-Umgebung geladen werden soll. Als letzte Möglichkeit wird die Datei `/etc/X11/xinit/Xclients` verwendet, um eine Desktop-Umgebung oder einen Window Manager zu wählen, der auf die gleiche Weise wie in Runlevel 3 benutzt wird.

Wenn der Benutzer eine X-Sitzung in der Standardanzeige beendet (`:0`) und sich abmeldet, wird das Skript `/etc/X11/xdm/TakeConsole` ausgeführt und weist dem root die Konsole neu zu. Der ursprüngliche Display Manager, der nach der Anmeldung weiter ausgeführt wurde, übernimmt die Steuerung und erzeugt einen neuen Display Manager. Auf diese Weise wird der XFree86-Server neu gestartet, ein neuer Anmeldebildschirm angezeigt und der gesamte Prozess neu gestartet.

Wenn sich der Benutzer aus X (Runlevel 5) abmeldet, wird dieser sich wieder im Display Manager befinden.

Für weitere Informationen darüber, wie Display Manger die Benutzerauthentifizierung steuern, sehen Sie die Datei /usr/share/doc/gdm-*<version-number>*/README (wobei *<version-number>* die Versionsnummer des installierten `gdm`-Pakets ist) und die `xdm` man-Seiten.

7.6. Zusätzliche Ressourcen

Über den XFree86-Server, die damit verbundenen Clients und die entsprechenden Desktop-Umgebungen sowie Window Manager ist noch lange nicht alles gesagt. Für erfahrene Benutzer können daher die zusätzlichen Ressourcen von großem Nutzen sein.

7.6.1. Installierte Dokumentation

- `/usr/X11R6/lib/X11/doc/README` — Beschreibt kurz die XFree86-Architektur und wie Einsteiger zusätzliche Informationen über das XFree86-Projekt erhalten.
- `>/usr/X11R6/lib/X11/doc/RELNOTES` — Für erfahrene Benutzer, die sich über die Neuheiten von XFree86 informieren möchten.
- `man XF86Config` — Enthält Informationen über die Konfigurationsdateien von XFree86, einschließlich der Bedeutung und der Syntax für die verschiedenen Abschnitte innerhalb der Dateien.
- `man XFree86` — Die wichtigste man-Seite für alle Informationen in Bezug auf XFree86. Hier werden der Unterschied zwischen den X-Serververbindungen auf lokaler Ebene und über ein Netzwerk detailliert beschrieben, übliche Umgebungsvariablen dargestellt, Optionen von Befehlszeilen erläutert und hilfreiche administrative Schlüsselkombinationen gegeben.
- `man Xserver` — Beschreibt den X Display Server.

7.6.2. Nützliche Webseiten

- http://www.xfree86.org/ — Die Home-Page des XFree86-Projekts, die die XFree86 Open Source-Version des X-Window-Systems bietet. XFree 86 steuert gemeinsam mit Red Hat Enterprise Linux die notwendige Hardware und stellt die grafische Umgebung zur Verfügung.
- http://sourceforge.net/projects/dri/ — Home-Page des DRI-Projekts (Direct Rendering Infrastructure). DRI ist die wesentliche 3D-Hardwarebeschleunigungskomponente von XFree86.
- http://www.redhat.com/mirrors/LDP/HOWTO/XFree86-HOWTO/ — Ein HOWTO-Dokument mit einer detaillierten Beschreibung der manuellen Installation und der benutzerdefinierten Konfiguration von XFree86.
- http://www.gnome.org/ — Home-Page des GNOME Projekts.
- http://www.kde.org/ — Home-Page für die KDE Desktop-Umgebung.
- http://nexp.cs.pdx.edu/fontconfig/ — Home-Page des Fontconfig Font-Subsystems für XFree86.

7.6.3. Zusätzliche Literatur

- *The Concise Guide to XFree86 for Linux* von Aron Hsiao; Que — Der Kommentar eines Experten über die Funktionsweise von XFree86 auf Linux-Systemen.
- *The New XFree86* von Bill Ball; Prima Publishing — Liefert einen guten und umfassenden Überblick über XFree86 in Zusammenhang mit den beliebtesten Desktop-Umgebungen wie GNOME und KDE.
- *Beginning GTK+ and GNOME* von Peter Wright; Wrox Press, Inc. — Eine Einführung für Programmierer in GNOME-Architektur und eine Erläuterung von GTK+.
- *GTK+/GNOME Application Development* von Havoc Pennington; New Riders Publishing — Fortgeschrittene Kenntnisse der GTK+-Programmierung, insbesondere über den Sample-Code und verfügbare APIs.
- *KDE 2.0 Development* von David Sweet und Matthias Ettrich; Sams Publishing — Leitet noch unerfahrene und erfahrene Entwickler an, wie die vielen Umgebungsrichtlinien am besten genutzt werden können, um QT-Anwendungen für KDE zu erstellen.

II. Hinweise für Netzwerk-Dienste

Unter Red Hat Enterprise Linux ist es möglich eine große Anzahl von Netzwerk-Diensten laufen zu lassen. Dieser Abschnitt beschreibt wie Netzwerk-Schnittstellen konfiguriert werden. Zusätzlich sind Details über kritische Netzwerk-Dienste, wie FTP, NFS, Apache HTTP Server, Sendmail, Postfix, Fetchmail, Procmail, BIND und LDAP vorhanden.

Inhaltsverzeichnis

8. Netzwerk-Schnittstellen. 107
9. Netzwerk-Dateisystem (Network File System - NFS) 119
10. Apache HTTP Server 131
11. Berkeley Internet Name Domain (BIND) 167
12. Lightweight Directory Access Protocol (LDAP) 187

redhat.

Kapitel 8.

Netzwerk-Schnittstellen

Bei der Verwendung von Red Hat Enterprise Linux verläuft die gesamte Netzwerkkommunikation zwischen konfigurierten Software-*Schnittstellen* und den *physischen Netzwerkgeräten*, die mit dem System verbunden sind.

Die Konfigurationsdateien für die verschiedenen Netzwerkschnittstellen und die Skripts zu deren Aktivierung oder Deaktivierung befinden sich im `/etc/sysconfig/network-scripts/`-Verzeichnis. Die bestimmten Schnittstellendateien können je nach System zwar unterschiedlich sein, es gibt aber grundsätzlich drei verschiedene Dateitypen in diesem Verzeichnis:

- *Schnittstellenkonfigurationsdateien*
- *Schnittstellenkontrollskripte*
- *Netzwerkfunktionsdateien*

Die Dateien in jeder dieser Kategorien arbeiten zusammen, um es zu ermöglichen auf die verschiedenen Netzwerkgeräte zurückzugreifen.

Dieses Kapitel beschäftigt sich mit den Verbindungen zwischen diesen Dateien und ihrer Verwendungsweise.

8.1. Netzwerk-Konfigurationsdateien

Bevor wir die Schnittstellen-Konfigurationsdateien tiefergehend untersuchen, wollen wir die zur Netzwerk-Konfiguration verwendeten primären Konfigurationsdateien auflisten. Das Verständnis der Rolle, die diese Dateien bei der Einrichtung des Netzwerk-Stack spielen, kann beim benutzerdefinieren eines Red Hat Enterprise Linux Systems nützlich sein.

Folgende sind primäre Netzwerk-Konfigurationsdateien:

- `/etc/hosts` — Hauptzweck dieser Datei ist es, Host-Namen zu lösen, die nicht anderweitig gelöst werden können. Sie kann auch zur Lösung von Host-Namen auf kleineren Netzwerken ohne DNS-Server verwendet werden. Unabhängig davon, an welchem Netzwerk der Computer angeschlossen ist, sollte diese Datei eine Zeile enthalten, die die IP-Adresse des Loopback-Gerätes (`127.0.0.1`) als `localhost.localdomain` angibt. Weitere Informationen finden in den man-Seiten zu `hosts`.
- `/etc/resolv.conf` — diese Datei gibt die IP-Adressen von DNS-Servern und die Search-Domain an. Wenn nicht anders konfiguriert, wird diese Datei von Initialisierungs-Skripten gefüllt. Weitere Informationen zu dieser Datei finden Sie auf den man-Seiten von `resolv.conf`.
- `/etc/sysconfig/network` — gibt Routing- und Host-Informationen für alle Netzwerk-Schnittstellen an. Weitere Informationen zu dieser Datei und darüber, welche Anweisungen sie akzeptiert, finden Sie unter Abschnitt 4.1.22.
- `/etc/sysconfig/network-scripts/ifcfg-<interface-name>` — für jede Netzwerk-Schnittstelle gibt es ein entsprechendes Schnittstellen-Konfigurationsskript. Jede dieser Dateien liefert Informationen, die für eine besondere Netzwerk-Schnittstelle spezifisch sind. Unter Abschnitt 8.2 finden Sie weitere Informationen zur Art der Datei und welche Anweisungen sie akzeptiert.

Achtung

Das Verzeichnis `/etc/sysconfig/networking/` wird vom **Network Administration Tool** (`redhat-config-network`) verwendet, und dessen Inhalt sollte nicht manuell bearbeitet werden. Weitere Informationen zur Konfiguration von Netzwerk-Schnittstellen anhand von **Network Administration Tool** finden Sie im Kapitel *Netzwerk-Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

8.2. Schnittstellen-Konfigurationsdateien

Schnittstellen-Konfigurationsdateien steuern die Software-Schnittstellen der einzelnen Netzwerkschnittstellengeräte. Wenn das System bootet, verwendet es diese Dateien, um zu erfahren, welche Schnittstellen automatisch gestartet werden und wie diese zu konfigurieren sind. Diese Dateien heißen normalerweise `ifcfg <Gerät>`, wobei `<Gerät>` sich auf den Namen des Geräts bezieht, das von der Konfigurationsdatei gesteuert wird.

8.2.1. Ethernet- Schnittstellen

Zu den am meisten verwendeten Schnittstellendateien gehört auch `ifcfg-eth0`, mit der die erste Ethernet *Netzwerk-Schnittstellen-Karte* im System, auch *NIC* genannt, gesteuert wird. In einem System mit mehreren NICs gibt es entsprechend mehrere `ifcfg eth<X>` Dateien (wobei `<X>` eine eindeutige Nummer ist, je nach der entsprechenden Schnittstelle). Da jedes Gerät über eine eigene Konfigurationsdatei verfügt, können Sie die Funktionalität jeder einzelnen Schnittstelle steuern.

Nachfolgend ist eine `ifcfg-eth0`-Beispielsdatei für ein System mit einer festen IP-Adresse:

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.1.0
NETMASK=255.255.255.0
IPADDR=10.0.1.27
USERCTL=no
```

Die in einer Schnittstellen-Konfigurationsdatei benötigten Werte können sich auf der Grundlage von anderen Werten ändern. Die `ifcfg-eth0`-Datei für eine Schnittstelle mit DHCP sieht beispielsweise etwas anders aus, weil die IP-Information vom DHCP-Server zur Verfügung gestellt wird:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Network Administration Tool (`redhat-config network`) macht es recht einfach, in den verschiedenen Schnittstellen-Konfigurationsdateien Änderungen vorzunehmen (Anleitungen zur Verwendung dieses Tools finden Sie im Kapitel *Netzwerk-Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*).

Sie können die Konfigurationsdateien für eine bestimmte Netzwerkschnittstelle auch manuell bearbeiten.

Folgend ist eine Liste mit konfigurierbaren Parametern für eine Konfigurationsdatei einer Ethernet-Schnittstelle:

- `BOOTPROTO=<Protokoll>`, wobei `<Protokoll>` für eine der folgenden Varianten stehen kann:
  - `none` — Es sollte kein Boot-Time-Protokoll verwendet werden.

  - `bootp` — Das BOOTP-Protokoll sollte verwendet werden.
  - `dhcp` — Das DHCP-Protocoll sollte verwendet werden.

- `BROADCAST=<Adresse>`, wobei `<Adresse>` für die Broadcast-Adresse steht. Diese Anweisung wird missbilligt.
- `DEVICE=<Name>`, wobei `<Name>` der der Name des physischen Geräts ist (ausgenommen dynamisch-zugewiesene PPP- Geräte, bei denen es der *logische Name*) ist.
- `DHCP_HOSTNAME` — Benutzen Sie diese Option lediglich, wenn der DHCP-Server den Client erfordert vor dem Erhalten einer IP-Adresse einen Hostnamen anzugeben. (Der DHCP-Server-Daemon in Red Hat Enterprise Linux unterstützt dieses Feature nicht.)
- `DNS{1,2}=<Adresse>`, wobei `<Adresse>` eine Name-Server-Adresse ist, die in `/etc/resolv.conf` gesetzt wird, wenn die Anweisung `PEERDNS` auf `yes` steht.
- `HWADDR=<MAC-address>`, wobei `<MAC-address>` die Hardware-Adresse des Ethernet-Geräts ist. Diese hat das Format `AA:BB:CC:DD:EE:FF`. Diese Anweisung ist für Rechner mit mehreren NICs nützlich, um sicherzustellen, dass die Schnittstellen den richtigen Gerätenamen zugewiesen werden, unabhängig von der Lade-Reihenfolge der NIC-Module. Diese Anweisung sollte *nicht* in Verbindung mit `MACADDR` verwendet werden.
- `IPADDR=<Adresse>`, wobei `<Adresse>` die IP-Adresse ist.
- `MACADDR=<MAC-address>`, wobei `<MAC-address>` die Hardware-Adresse des Ethernet-Geräts ist. Diese hat das Format `AA:BB:CC:DD:EE:FF`. Diese Anweisung wird verwendet um einer Schnittstelle eine MAC-Adresse zuzuweisen, wobei die der physischen NIC überschrieben wird. Diese Anweisung sollte *nicht* in Verbindung mit `HWADDR` verwendet werden.
- `MASTER=<bond-interface>`, wobei `<bond-interface>` das Channel-Bonding-Interface ist, zu dem die Ethernet-Schnittstelle verbunden ist.

  Diese Anweisung wird zusammen mit der `SLAVE`-Anweisung verwendet.

  Sehen Sie Abschnitt 8.2.3 für Weiteres zu Channel-Bonding-Interfaces.
- `NETMASK=<Maske>`, wobei `<Make>` der Wert der Netzmaske ist.
- `NETWORK=<Adresse>`, wobei `<Adresse>` die Netzwerkadresse ist. Diese Anweisung wird nicht länger verwendet.
- `ONBOOT=<Antwort>`, wobei `<Antwort>` Folgendes bedeuten kann:
  - `yes` — Dieses Gerät sollte beim Booten aktiviert werden.
  - `no` — Dieses Gerät sollte nicht beim Booten aktiviert werden.

- `PEERDNS=<Antwort>`, wobei `<Antwort>` Folgendes bedeuten kann:
  - `yes` — Ändern Sie `/etc/resolv.conf`, wenn die DNS-Anweisung gesetzt ist. Verwenden Sie DCHP, dann ist `yes` Standard.
  - `no` — ändern Sie `/etc/resolv.conf` nicht.

- `SLAVE=<bond-interface>`, wobei `<bond-interface>` Folgendes bedeuten kann:
  - `yes` — Dieses Gerät wird vom in der `MASTER`-Direktive angegebenen Channel-Bonding-Interface gesteuert.
  - `no` — Dieses Gerät wird *nicht* vom in der `MASTER`-Direktive angegebenen Channel-Bonding-Interface gesteuert.

  Diese Anweisung wird zusammen mit der `MASTER`-Anweisung verwendet.

Sehen Sie Abschnitt 8.2.3 für Weiteres zu Channel-Bonding-Interfaces.

- `SRCADDR=<Adresse>`, wobei `<Adresse>` die angegebene Ausgangs-IP-Adresse für ausgehende Pakete ist.
- `USERCTL=<Antwort>`, wobei `<Antwort>` Folgendes bedeuten kann:
  - `yes` — Nicht-root dürfen dieses Gerät kontrollieren.
  - `no` — Nicht-root dürfen dieses Gerät nicht kontrollieren.

8.2.2. IPsec Schnittstellen

Mit Red Hat Enterprise Linux ist es möglich zu anderen Hosts oder Netzwerken über eine sichere IP-Verbindung, als IPsec bekannt, zu verbinden. Anleitungen zur Einrichtung einer IPsec-Verbindung mit **Network Administration Tool** (`redhat-config-network`) sehen Sie das Kapitel *Netzwerk-Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*. Für das manuelle Einrichten von IPsec-Verbindungen, sehen Sie das Kapitel *Virtuelle Private Netzwerke* im *Red Hat Enterprise Linux Sicherheitshandbuch*.

Die Folgende ist die Datei `ifcfg` für eine Netzwerk-zu-Netzwerk IPsec-Verbindung für LAN A. Der eindeutige Name, mit dem die Verbindung in diesem Beispiel identifiziert wird ist `ipsec1`, weswegen die entsprechende Datei `/etc/sysconfig/network-scripts/ifcfg-ipsec1` ist.

```
TYPE=IPsec
ONBOOT=yes
IKE_METHOD=PSK
SRCNET=192.168.1.0/24
DSTNET=192.168.2.0/24
DST=X.X.X.X
```

In diesem Beispiel ist `X.X.X.X` die öffentliche IP-Adresse des Ziel-IPsec-Routers.

Folgend ist eine Liste mit konfigurierbaren Parametern für eine IPsec-Schnittstelle:

- `DST=<address>`, wobei `<address>` die IP-Adresse des IPsec Ziel-Host oder Router ist. Dies wird sowohl für Host-zu-Host, als auch für Netzwerk-zu-Netzwerk IPsec-Konfigurationen verwendet.
- `DSTNET=<network>`, wobei `<network>` die Netzwerk-Adresse des IPsec Ziel-Netzwerks ist. Dies wird lediglich für Netzwerk-zu-Netzwerk IPsec-Konfigurationen verwendet.
- `SRC=<address>`, wobei `<address>` die IP-Adress des IPsec Quellen-Host oder Router ist. Diese Einstellung ist optional und wird lediglich für Host-zu-Host IPsec-Konfigurationen verwendet.
- `SRCNET=<network>`, wobei `<network>` die Netzwerk-Adresse des IPsec Ziel-Netzwerks ist. Dies wird lediglich für Netzwerk-zu-Netzwerk IPsec-Konfigurationen verwendet.
- `TYPE=<interface-type>`, wobei `<interface-type>` `IPSEC` ist.

Siehe `/usr/share/doc/initscripts-<version-number>/sysconfig.txt` (ersetze `<version-number>` mit der Version des installierten `initscripts`-Pakets) für Konfigurationsparameter, wenn manuelle Key-Verschlüsselung mit IPsec verwendet wird.

Wenn `racoon` verwendet wird, um Key-Verschlüsselung automatisch zu verwalten, sind folgende Optionen erfordert:

- `IKE_METHOD=<encryption-method>`, wobei `<encryption-method>` entweder `PSK`, `X509` oder `GSSAPI` ist. Wenn `PSK` angegeben ist, muss der `IKE_PSK`-Parameter gesetzt sein. Wenn `X509` angegeben ist, muss der `IKE_CERTFILE`-Parameter auch gesetzt sein.
- `IKE_PSK=<shared-key>`, wobei `<shared-key>` der gemeinsame, geheime Wert für die PSK (Preshared Keys) Methode ist.
- `IKE_CERTFILE=<cert-file>`, wobei `<cert-file>` eine gültige X.509 Zertifikatsdatei für den Host ist.
- `IKE_PEER_CERTFILE=<cert-file>`, wobei `<cert-file>` eine gültige X.509 Zertifikatsdatei für den *Remote*-Host ist.
- `IKE_DNSSEC=<answer>`, wobei `<answer>` `yes` ist. Der `racoon`-Daemon empfängt das X.509 Zertifikat des Remote-Host über DNS. Wenn ein `IKE_PEER_CERTFILE` angegeben ist, schließen Sie diesen Parameter *nicht* ein.

Für weitere Informationen zu Verschlüsselungsalgorithmen, die für IPsec verfügbar sind, sehen Sie die `setkey` man-Seite. Für weitere Informationen zu `racoon`, sehen Sie `racoon` und die `racoon.conf` man-Seiten.

8.2.3. Channel-Bonding-Schnittstellen

Red Hat Enterprise Linux erlaubt Administratoren mehrere Netzwerk-Schnittstellen in einem einzelnen Kanal zusammenzuführen, indem die `bonding` Kernelmodule und eine spezielle Netzwerk-Schnitstelle, Channel-Bonding-Interface genannt, verwendet werden. Channel Bonding erlaubt es mehreren Netzwerk-Schnittstellen als eine zu arbeiten, die Bandbreite zu erhöhen und Redundanz zu gewähren.

Um ein Channel-Bonding-Interface zu erstellen, erzeugen Sie eine Datei im Verzeichnis `/etc/sysconfig/network-scripts/` mit dem Namen `ifcfg-bond<N>`, wobei Sie `<N>` mit der Nummer der Schnittstelle, z.B. `0`, ersetzen.

Der Inhalt der Datei kann dem Typ der Schnittstelle entsprechen, die in einem Channel-Bonding-Interface verwendet wird, wie einer Ethernet-Schnittstelle. Der einzige Unterschied ist, dass die `DEVICE=`-Direktive auf `bond<N>` gesetzt werden muss, wobei `<N>` die Nummer der Schnittstelle ist.

Die Folgende ist ein Beispiel einer Channel-Bonding Konfigurationsdatei:

```
DEVICE=bond0
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.1.0
NETMASK=255.255.255.0
IPADDR=10.0.1.27
USERCTL=no
```

Nachdem das Channel-Bonding-Interface erzeugt wurde, müssen die zu bindenden Netzwerk-Schnittstellen konfiguriert werden, indem die `MASTER=`-und `SLAVE=`-Anweisungen zu deren Konfigurationsdateien hinzugefügt werden. Die Konfigurationdateien der gebundenen Schnittstellen können fast identisch sein.

Wenn, zum Beispiel, zwei Ethernet-Schnittstellen gebunden werden, können beide, `eth0` und `eth1`, wie im folgenden Beispiel aussehen:

```
DEVICE=eth<N>
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

```
USERCTL=no
```

In diesem Beispiel steht <*N*> für die Nummer der Schnittstelle.

Damit ein Channel-Bonding-Interface gültig ist, muss das Kernelmodul geladen sein. Um sicherzustellen, dass das Kernelmodul geladen ist, wenn das Channel-Bonding-Interface hochgefahren wird, muss folgende Zeile zur Datei `/etc/modules.conf` hinzugefügt werden:

```
alias bond<N> bonding
```

<*N*> steht hierbei für die Nummer der Schnittstelle, wie `0`. Für jedes konfigurierte Channel-Bonding-Interface muss ein entsprechender Eintrag in der Datei `/etc/modules.conf` stehen.

Ist `/etc/modules.conf`, das Channel-Bonding-Interface und sind die Netzwerk-Schnittstellen erst einmal konfiguriert, kann der Befehl `ifup` verwendet werden, um das Channel-Bonding-Interface hochzufahren.

Wichtig

Wichtige Aspekte des Channel-Bonding-Interface werden durch das Kernelmodul kontrolliert. Für weitere Informationen zur Kontrolle der `bonding`-Module, sehen Sie Abschnitt A.3.2.

8.2.4. Alias- und Clone-Dateien

Zwei weniger verwendete Arten von Schnittstellen-Konfigurationsdateien sind *Alias-* und *Clone* Dateien.

Alias-Schnittstellen-Konfigurationsdateien haben das Format `ifcfg-<if-name>:<alias-value>`. Diese werden hauptsächlich verwendet, um mehrere Adressen zu einer einzelnen Schnittstelle zu binden.

Eine `ifcfg-eth0:0`-Datei kann z.B. so konfiguriert werden, dass sie `DEVICE=eth0:0` und eine statische IP-Adresse 10.0.0.2 spezifieren kann und somit als Alias einer bereits konfigurierten Ethernet-Schnittstelle dienen kann, um ihre IP- Informationen über DHCP in `ifcfg-eth0` zu empfangen. An dieser Stelle ist das `eth0`-Gerät mit einer dynamischen IP-Adresse verknüpft, kann aber jederzeit über die feste 10.0.0.2 IP-Adresse auf das System zurückgreifen.

Achtung

Alias-Schnittstellen unterstützen DHCP nicht.

Bei der Namensgebung einer Clone-Schnittstellen-Konfigurationsdatei sollten folgende Konventionen eingehalten werden: `ifcfg-<if-name>-<clone-name>`. Während mit einer Alias-Datei auf eine bereits bestehende Schnittstellen-Konfigurationsdatei zurückgegriffen werden kann, wird eine Clone-Datei zum Festlegen zusätzlicher Optionen während der Angabe einer Schnittstelle verwendet. Die standardmäßige DHCP Ethernet-Schnittstelle mit dem Namen `eth0` kann deshalb wie folgt oder ähnlich aussehen:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
```

Da `USERCTL` auf `no` eingestellt ist, können Benutzer, wenn nichts anderes angegeben wird, diese Schnittstelle nicht starten oder beenden. Um den Benutzern dies zu ermöglichen, erstellen Sie einen Clone durch Kopieren von `ifcfg-eth0` nach `ifcfg-eth0-user` und fügen Sie folgende Zeile zu `ifcfg-eth0-user` hinzu:

```
USERCTL=yes
```

Wenn ein Benutzer mit dem Befehl `/sbin/ifup eth0-user` die `eth0`-Schnittstelle startet, werden die Konfigurationsoptionen von `ifcfg-eth0` und `ifcfg-eth0-user` kombiniert. Dies ist zwar nur ein sehr einfaches Beispiel, diese Methode kann über für viele verschiedene Optionen und Schnittstellen verwendet werden.

Der einfachste Weg zur Erstellung von Alias- und Clone-Schnittstellen-Konfigurationsdateien ist die Verwendung des grafischen **Network Administration Tool**. Weitere Informationen zur Verwendung dieses Tools finden Sie im Kapitel *Netzwerk-Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

8.2.5. Schnittstellen für den Verbindungsaufbau

Wenn Sie über einen Dialup-Account mit dem Internet verbinden, brauchen Sie eine Konfigurationsdatei für diese Schnittstelle.

PPP-Schnittstellendateien haben das Format `ifcfg-ppp<X>` (wobei *<X>* eine eindeutige, einer spezifischen Schnittstelle entsprechende Nummer ist).

Die Konfigurationsdatei der PPP-Schnittstelle wird automatisch erzeugt, wenn Sie `wvdial`, **Network Administration Tool** oder **Kppp** verwenden, um einen Dialup-Account zu erzeugen. Sie können diese Datei aber auch manuell erstellen und bearbeiten.

Folgend ist eine typische `ifcfg-ppp0`-Datei:

```
DEVICE=ppp0
NAME=test
WVDIALSECT=test
MODEMPORT=/dev/modem
LINESPEED=115200
PAPNAME=test
USERCTL=true
ONBOOT=no
PERSIST=no
DEFROUTE=yes
PEERDNS=yes
DEMAND=no
IDLETIMEOUT=600
```

Serial Line Internet Protocol (SLIP) ist eine weitere Dialup-Schnittstelle, wird im allgemeinen aber seltener verwendet. Ein typischer Name für die Schnittstellen-Konfigurationsdatei der SLIP-Dateien ist z.B. `ifcfg-sl0`.

Folgende Optionen können in diesen Dateien verwendet werden:

- `DEFROUTE=<Antwort>`, wobei *<Antwort>* Folgendes bedeuten kann:
  - `yes` — Stellt diese Schnittstelle als Standardroute ein.
  - `no` — Stellt diese Schnittstelle nicht als Standardroute ein.

- `DEMAND=<Antwort>`, wobei *<Antwort>* Folgendes bedeuten kann:

  - `yes` — Mit dieser Schnittstelle kann `pppd` eine Verbindung starten, wenn darauf zugegriffen wird.
  - `no` — Verbindungen mit dieser Schnittstelle müssen manuell hergestellt werden.

- `IDLETIMEOUT=<Wert>`, wobei `<Wert>` die Sekunden ohne Aktivität darstellt, nach denen die Schnittstelle die Verbindung selbst unterbricht.
- `INITSTRING=<Zeichenkette>`, wobei `<Zeichenkette>` die erste Zeichenfolge ist, die an das Modem übergeben wird. Diese Option wird hauptsächlich von SLIP-Schnittstellen verwendet.
- `LINESPEED=<Wert>`, wobei `<Wert>` die Baudrate des Gerätes angibt. Zu den möglichen Standardwerten gehören `57600`, `38400`, `19200` und `9600`.
- `MODEMPORT=<Gerät>`, wobei `<Gerät>` der Name des Serial-Geräts ist, das die Verbindung für die Schnittstelle herstellt.
- `MTU=<Wert>`, wobei `<Wert>` die *Maximum Transfer Unit (MTU)*-Einstellung für die Schnittstelle ist. Die MTU bezieht sich auf die größtmögliche Zahl von Daten (in Bytes), die ein Frame übertragen kann, die Header-Information nicht mitgezählt. Bei einigen Dial-up-Situationen hat die Einstellung dieses Werts auf `576` zur Folge, dass weniger Pakete ausgelassen werden (DROP) und die Durchlässigkeit für Verbindungen leicht erhöht wird.
- `NAME=<Name>`, wobei `<Name>` sich auf den Oberbegriff der Konfigurationssammlung für Dialup-Verbindungen bezieht.
- `PAPNAME=<Name>`, wobei `<Name>` für den Benutzernamen steht, der während der Änderung des *Password Authentication Protocol (PAP)* vergeben wurde und Ihnen die Verbindung zu einem Remote-System ermöglicht.
- `PERSIST=<Antwort>`, wobei `<Antwort>` Folgendes bedeuten kann:
  - `yes` — Diese Schnittstelle sollte ständig aktiviert sein, auch wenn nach einem Abbruch das Modem deaktiviert wird.
  - `no` — Diese Schnittstelle sollte nicht ständig aktiv sein.

- `REMIP=<Adresse>`, wobei `<Adresse>` die IP-Adresse des Remote-Systems ist. Wird üblicherweise nicht festgelegt.
- `WVDIALSECT=<Name>`, wobei `<Name>` dieser Schnittstelle in `/etc/wvdial.conf` eine Anwähl-Konfiguration zuweist, die die anzuwählende Telefonnummer und andere wichtige Informationen für die Schnittstelle enthält.

8.2.6. Weitere Schnittstellen

Weitere übliche Schnittstellen-Konfigurationsdateien, die diese Optionen verwenden, sind die folgenden:

- `ifcfg-lo` — Ein lokale *Loopback-Schnittstelle* wird oft zum Testen verwendet, wie auch in Applikationen, die eine zum System zurückweisende IP-Adresse benötigen. Jegliche Daten, die zum Loopback-Gerät gesendet werden, werden augenblicklich zur Netzwerkschicht des Host zurückgegeben.

Warnung

Bearbeiten Sie niemals das Loopback-Schnittstellenskript `/etc/sysconfig/network-scripts/ifcfg-lo` von Hand. Andernfalls kann die richtige Funktionsweise des Systems beeinträchtigt werden.

- `ifcfg-irlan0` — Eine *Infrarot-Schnittstelle* sorgt dafür, dass Informationen zwischen Geräten wie Laptop und Drucker über einen Infrarot-Link fließen, welcher ähnlich arbeitet wie ein Ethernet-Gerät, mit dem Unterschied, dass es normalerweise über eine Peer-to-Peer-Verbindung läuft.
- `ifcfg-plip0` — Eine *Parallel-Line-Interface-Protocol (PLIP)*-Verbindung arbeitet auf ähnliche Weise, mit dem Unterschied, dass sie eine parallelen Schnittstelle verwendet.
- `ifcfg-tr0` — *Token Ring* Topologien sind nicht mehr so verbreitet auf *Local Area Networks* (*LANs*), da sie durch Ethernet verdrängt wurden.

8.3. Schnittstellen-Kontrollskripts

Die Schnittstellen-Kontrollskripts aktivieren und deaktivieren Systemschnittstellen. Die zwei wichtigsten Schnittstellen-Kontroll-Skripts sind `/sbin/ifdown` und `/sbin/ifup`, die verschiedene andere Kontrollskripte aus dem `/etc/sysconfig/network scripts/`-Verzeichnis verwenden.

`ifup` und `ifdown` sind symbolische Links zu den Skripte im `/sbin/`-Verzeichnis. Wenn eines der beiden Skripte aufgerufen wird, verlangt dieses, dass ein Schnittstellenwert angegeben wird, wie z.B.:

```
ifup eth0
```

Achtung

`ifup` und `ifdown` sind die einzigen Skripte, die der Benutzer zum Starten und Beenden der Netzwerk-Schnittstellen verwenden sollte.

Die folgenden Skripte sind lediglich zu Referenzzwecken angegeben.

An dieser Stelle werden zwei Dateien, `/etc/rc.d/init.d/functions` und `/etc/sysconfig/network-scripts/network-functions` dazu verwendet, eine ganze Reihe von Aufgaben der Initialisierung des Netzwerks zu erfüllen. Weitere Informationen finden Sie unter Abschnitt 8.4.

Nachdem sichergestellt ist, dass eine Schnittstelle angegeben wurde und dass der Benutzer, der diese Anfrage ausführt, die Berechtigung zur Steuerung der Schnittstelle hat, wird das richtige Skript zum Starten oder Beenden der Schnittstelle aufgerufen. Zu den gängigsten Schnittstellen-Kontrollskripten im Verzeichnis `/etc/sysconfig/network-scripts/` gehören die Folgenden:

- `ifup-aliases` — Konfiguriert die IP-Aliase der Schnittstellen-Konfigurationsdateien, wennn einer Schnittstelle mehr als eine IP-Adresse zugeordnet ist.
- `ifup-cipcb` und `ifdown-cipcb` — Werden zum Starten und Beenden von *Crypto IP Encapsulation (CIPE)*-Verbindungen verwendet.
- `ifup-ipv6` und `ifdown-ipv6` — Werden zum Starten oder Beenden einer IPv6-Schnittstelle verwendet.
- `ifup-ipx` — Wird zum Starten einer IPX-Schnittstelle verwendet.
- `ifup-plip` — Wird zum Starten einer PLIP-Schnittstelle verwendet.
- `ifup-plusb` — Wird zum Starten einer USB-Schnittstelle für Netzwerkverbindungen verwendet.
- `ifup-post` und `ifdown-post` — Enthalten Befehle, die nach dem Starten oder Beenden einer Schnittstelle ausgeführt werden müssen.

- `ifup-ppp` und `ifdown-ppp` — Werden zum Starten oder Beenden einer PPP-Schnittstelle verwendet.
- `ifup-routes` — Fügt statische Routes für ein bestimmtes Gerät hinzu, wenn dessen Schnittstelle aktiviert wird.
- `ifdown-sit` und `ifup-sit` — Enthalten eine Funktion, die zum Aktivieren und Deaktivieren eines IPv6- Tunnels in einer IPv4-Verbindung aufgerufen wird.
- `ifup-sl` und `ifdown-sl` — Wird zum Starten und Beenden einer SLIP Schnittstelle verwendet.

Warnung

Achten Sie darauf, dass das Entfernen oder Modifizieren irgendeines Skripts im Verzeichnis `/etc/sysconfig/network-scripts/` dazu führen kann, dass Schnittstellenverbindungen seltsam reagieren oder scheitern, da sie von diesen Skripts abhängig sind. Nur erfahrene Benutzer sollten daher Skripts verändern, die für eine Netzwerkschnittstelle relevant sind.

Der einfachste Weg, alle Netzwerk-Skripte gleichzeitig zu ändern ist es, den Befehl `/sbin/service` auf dem Netzwerk-Service (`/etc/rc.d/init.d/network`) wie folgt auszuführen:

```
/sbin/service network <action>
```

<*Aktion*> steht entweder für `start`, `stop` oder `restart`.

Um eine Liste der konfigurierten Geräte und der augenblicklich aktiven Netzwerk-Schnittstellen anzuzeigen, benutzen Sie folgenden Befehl:

```
/sbin/service network status
```

8.4. Netzwerkfunktionsdateien

Red Hat Enterprise Linux nutzt verschiedene Dateien, die wichtige allgemeine Funktionen zum aktivieren und deaktivieren von Schnittstellen enthalten. Diese Funktionen werden in einigen wenigen Dateien in geeigneter Weise gruppiert und können bei Bedarf einfach abgerufen werden, wodurch diese Funktionen nicht in jeder Kontrolldatei enthalten sein müssen.

Die gängigste Netzwerkfunktionsdatei ist `/etc/sysconfig/network-scripts/network-functions`. Diese Datei enthält eine Vielzahl von allgemeinen IPv4-Funktionen, die für viele Schnittstellenkontrollskripte hilfreich sind. Hierzu gehört das Kontaktieren laufender Programme, die Informationen zu den Änderungen des Schnittstellenstatus benötigen, das Einrichten von Host-Namen, die Suche eines Gateway-Gerätes, das Prüfen, ob ein bestimmtes Gerät ausgefallen ist oder nicht, und das Hinzufügen einer Standard-Route.

Da die Funktionen, die für die IPv6-Schnittstellen benötigt werden, sich von denen für IPv4-Schnittstellen unterscheiden, gibt es eine Datei `/etc/sysconfig/network-scripts/network-functions-ipv6`, In dieser Datei finden Sie Funktionen, die statische IPv6-Routen konfigurieren und löschen, Tunnel erstellen und entfernen, IPv6-Adressen einer Schnittstelle hinzufügen oder sie von dort entfernen und Dateien zum Testen, ob auf der Schnittstelle eine IPv6-Adresse existiert.

8.5. Zusätzliche Ressourcen

Die Folgenden sind Ressourcen, die näher auf Netzwerk-Schnittstellen eingehen.

8.5.1. Installierte Dokumentation

- `/usr/share/doc/initscripts-<version>/sysconfig.txt` — Ein verständlicher Leitfaden zu verfügbaren Optionen für Netzwerk-Konfigurationsdateien, einschließlich IPv6-Optionen, die in diesem Kapitel nicht behandelt werden.
- `/usr/share/doc/iproute-<version>/ip-cref.ps` — Diese Datei enthält eine Vielzahl an Informationen zu `ip`, die u.a. zur Bearbeitung von Routing-Tabellen verwendet werden können. Sehen Sie sich diese Datei mit **ggv** oder **kghostview** an.

Kapitel 9.

Netzwerk-Dateisystem (Network File System - NFS)

Mit dem *Netzwerk-Dateisystem* (*NFS*) können Remote-Hosts Dateisysteme auf einem System mounten und verwenden, als wären sie lokal gemountet. Dies ermöglicht den Systemadministratoren, Ressourcen auf zentralen Servern im Netzwerk sicherzustellen.

Dieses Kapitel konzentriert sich auf fundamentale NFS-Konzepte und ergänzende Information. Für detaillierte Anweisungen bezüglich Konfiguration und Funktion von NFS-Servern und Client-Software siehe Kapitel *Network File System (NFS)* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

9.1. Wie es funktioniert

Zur Zeit werden zwei Versionen von NFS verwendet. Die Version 2 von NFS (NFSv2) ist älter, wird aber von vielen Systemen unterstützt. Die NFS-Version 3 (NFSv3) verfügt über mehr Features, einschließlich einer variablen Dateigröße und einem besseren Fehlerreport, ist aber mit NFSv2-Clients nicht vollständig kompatibel. Red Hat Enterprise Linux unterstützt sowohl NFSv2- als auch NFSv3-Clients, und wenn ein Dateisystem via NFS gemountet wird, verwendet Red Hat Enterprise Linux NFSv3 als Standard, wenn der Server es unterstützt.

NFSv2 verwendet das *User Datagram Protocol* (*UDP*) um eine Netzwerkverbindung ohne Statuszwischen dem Client und dem Server herzustellen. NFSv3 kann entweder UDP oder *Transmission Control Protocol* (*TCP*) verwenden, wenn es auf einem Netzwerk läuft.

Die statuslose UDP-Verbindung minimiert unter normalen Umständen den Netzwerkverkehr, da der NFS-Server dem Client ein Cookie sendet, nachdem der Client für den Zugriff auf die gemeinsamen Dateien autorisiert worden ist. Dieses Cookie ist ein zufälliger Wert, der im Server gespeichert ist und gemeinsam mit RPC-Anfragen vom Client übermittelt wird. Der NFS-Server kann ohne Auswirkung auf die Clients neu gestartet werden, das Cookie bleibt dabei intakt. Da aber UDP statuslos ist, bestürmen die UD- Clients das Netzwerk weiterhin mit Anfragen für den Server, auch wenn der Server unerwarteterweise herunterfährt. Deswegen ist TCP das bevorzugte Protokoll beim Verbinden mit einem NFSv3-Server.

Anmerkung

Aus Gründen der Kompatibilität ist UDP das standardmäßige Transport-Protokoll für NFS unter Red Hat Enterprise Linux. Siehe Kapitel *Network File System (NFS)* im *Red Hat Enterprise Linux Handbuch zur System-Administration* für weitere Informationen über Verbindung zum Server mittels TCP.

NFS führt Authentifizierungen nur dann durch, wenn ein Client versucht, die gemeinsame NFS-Ressource zu mounten. Um Zugriffe auf den NFS-Server zu limitieren werden TCP-Wrapper verwendet. Die TCP-Wrapper lesen die Dateien `/etc/hosts.allow` und `/etc/hosts.deny`, um festzulegen, ob einem bestimmten Client oder einem Netzwerk der Zugriff auf den NFS-Server erlaubt oder verwehrt wird. Weitere Informationen zum Konfigurieren der Zugriffssteuerung mit TCP-Wrapper finden Sie unter Kapitel 14.

Erhält der Client die Berechtigung, die TCP-Wrapper zu passieren, verweist der NFS-Server auf die Konfigurationsdatei `/etc/exports`, um festzulegen, ob der Client über ausreichende Privilegien zum Zugreifen auf eine der exportierten Dateisysteme verfügt. Wird der Zutritt gewährt, kann der User über alle Datei- und Verzeichnisvorgänge verfügen.

Warnung

NFS-Mount-Privilegien werden dem Client Host gewährt, nicht dem Benutzer. Deswegen kann jeder Benutzer auf einem Client Host mit Zugangsberechtigung auf die exportierten Dateisysteme zugreifen. Wenn Sie die gemeinsamen NFS- Dateien konfigurieren, seien Sie vorsichtig, welche Hosts eine Lese- und Schreibberechtigung erhalten (`rw`).

9.1.1. Erforderliche Dienste

Red Hat Enterprise Linux verwendet für das NFS Datei-Sharing eine Kombination aus dem Kernel-Level-Support und den Daemon-Prozessen. NFS verlässt sich auf *Remote Procedure Calls* (*RPC*), um Anfragen zwischen Clients und Servern zu routen. Bei Linux werden RPC-Dienste durch den `portmap` Dienst gesteuert. Beim gemeinsamen Verwenden oder mounten von NFS-Dateisystemen arbeiten folgende Dienste zusammen:

- `nfs` — Startet die passenden RPC-Prozesse, um Anfragen für gemeinsame NFS-Dateisysteme zu handhaben.
- `nfslock` — ein fakultativer Dienst, der die passenden RPC-Prozesse startet, damit NFS-Clients Dateien auf dem Server festmachen können.
- `portmap` — Der RPC-Dienst für Linux; er reagiert auf Anfragen für RPC-Dienste und und baut Verbindungen zu den erfragten RPC-Diensten auf

Die folgenden RPC-Prozesse arbeiten im Hintergrund zusammen, um die NFS-Dienste zu unterstützen:

- `rpc.mountd` — Dieser Prozess empfängt die Mount-Anfrage der NFS-Clients und kontrolliert, ob das erfragte Dateisystem zu diesem Zeitpunkt exportiert ist. Der Prozess wird automatisch durch den `nfs` Dienst gestartet und erfordert keine Benutzer- Konfiguration.
- `rpc.nfsd` — Dieser Prozess ist der NFS-Server. Er arbeitet mit dem Linux-Kernel, um mit den dynamischen Vorgaben des NFS-Clients übereinzustimmen. Zum Beispiel das Bereitstellen zusätzlicher Server-Threads, immer wenn sich ein NFS-Client verbindet. Dieser Prozess korrespondiert mit dem `nfs` Dienst.
- `rpc.lockd` — Ein fakultativer Prozess, der NFS-Clients erlaubt, Dateien am Server festzumachen. Dieser Prozess korrespondiert mit dem`nfslock` Dienst.
- `rpc.statd` — Implementiert das *Network Status Monitor (NSM)*-RPC- Protokoll. Dies verständigt NFS-Clients, wenn ein NFS-Server neu gestartet wird, ohne dass er ordentlich heruntergefahren wurde. Dieser Prozess wird automatisch durch den `nfslock` Dienst gestartet und erfordert keine Benutzer-Konfiguration.
- `rpc.rquotad` — Dieser Prozess stellt Information über Benutzerquoten für Remote-Benutzer zur Verfügung. Der Prozess wird automatisch durch den `nfs` Dienst gestartet und erfordert keine Benutzer-Konfiguration.

9.1.2. NFS und `portmap`

Der `portmap` Dienst von Linux wird benötigt, um die RPC-Anfragen den korrekten Dienste zuzuordnen. `portmap` wird von den RPC-Prozessen benachrichtigt, wenn sie starten. Des Weiteren teilen die Anfragen die überwachte Port-Nummer sowie die Nummern des RPS-Programms mit, die aufgerufen werden. Der Client kontaktiert `portmap` auf dem Server mit einer bestimmten RPC-Programmnummer. Der `portmap` Dienst leitet dann den Client zur richtigen Port-Nummer um, damit er mit dem gewünschten Dienst kommunizieren kann.

Da Dienste. die auf RPC-basieren, für die Verbindungen mit ankommenden Client-Anfragen von `portmap` abhängig sind, muss `portmap` verfügbar sein, bevor einer dieser Dienste gestartet wird.

Der `portmap`-Dienst verwendet TCP-Wrapper für die Zugriffskontrolle, die Zugriffs-Kontrollregeln für `portmap` beeinflussen *alle* auf RPC basierenden Dienste. Als Alternative können Sie auch Zugriffs-Kontrollregeln für jeden der NFS-RPC-Daemonen einzeln bestimmen. Die man-Seiten für `rpc.mountd` und `rpc.statd` enthalten Informationen über die genaue Syntax dieser Regeln.

9.1.2.1. Probemlösungen bei NFS mit `portmap`

Da `portmap` die Koordination zwischen RPC- Diensten und den Port-Nummern übernimmt, die für die Kommunikation mit den Diensten verwendet werden, ist es beim Lösen von Problemen sehr hilfreich, eine Übersicht über die aktuellen RPC- Dienste zu haben, die `portmap` verwenden. Der Befehl `rpcinfo` zeigt jeden auf RPC-basierenden Dienst mit Port-Nummern, RPC-Programmnummer, Version und dem Typ des IP- Protokolls (TCP oder UDP) an.

Um sicherzustellen, dass die richtigen NFS-RPC-basierten Dienste für `portmap` aktiviert sind, geben Sie den folgenden Befehl als Root ein:

```
rpcinfo -p
```

Im folgenden ein Probe-Output dieses Befehls:

```
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100021    1   udp  32774  nlockmgr
    100021    3   udp  32774  nlockmgr
    100021    4   udp  32774  nlockmgr
    100021    1   tcp  34437  nlockmgr
    100021    3   tcp  34437  nlockmgr
    100021    4   tcp  34437  nlockmgr
    100011    1   udp    819  rquotad
    100011    2   udp    819  rquotad
    100011    1   tcp    822  rquotad
    100011    2   tcp    822  rquotad
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100005    1   udp    836  mountd
    100005    1   tcp    839  mountd
    100005    2   udp    836  mountd
    100005    2   tcp    839  mountd
    100005    3   udp    836  mountd
    100005    3   tcp    839  mountd
```

Im oben aufgeführten Output wird angezeigt, dass die richtigen NFS-Dienste ausgeführt sind. Wenn einer der NFS-Dienste nicht korrekt startet, kann `portmap` die RPC-Anfragen von Clients für diesen Dienst nicht dem richtigen Port zuordnen. Wenn NFS im `rpcinfo` Output nicht vorhanden ist, führt in vielen Fällen das Neustarten von NFS dazu, dass der Dienst korrekt in `portmap` registriert werden und arbeiten kann. Anweisungen für das Starten von NFS finden Sie unter Abschnitt 9.2.

Andere hilfreiche Optionen sind für den `rpcinfo` Befehl vorhanden. Siehe `rpcinfo` man Seite für weitere Informationen.

9.2. Starten und Anhalten von NFS

Um einen NFS Server zu betreiben, muss der `portmap` Dienst ausgeführt sein. Um zu überprüfen, dass `portmap` aktiv ist, geben Sie den folgenden Befehl als Root ein:

```
/sbin/service portmap status
```

Wenn der`portmap` Dienst ausgeführt ist, dann kann der `nfs` Dienst gestartet werden. Um einen NFS-Server zu starten, geben Sie als Root ein:

```
/sbin/service nfs start
```

Um den Server anzuhalten, geben Sie als Root ein:

```
/sbin/service nfs stop
```

Die `restart` Option ist ein verkürzter Weg für das Anhalten und Starten von NFS. Dies ist der beste Weg, Änderungen an der Konfiguration wirksam werden zu lassen, wenn die Konfigurationsdateien von NFS bearbeitet wurden.

Um den Server neu zu starten, geben Sie als Root ein:

```
/sbin/service nfs restart
```

Die `condrestart` (*conditional restart*) Option startet `nfs` nur, wenn es zu diesem Zeitpunkt ausgeführt ist. Diese Option ist für Skripts hilfreich, weil sie den Deamon nicht startet, wenn er nicht ausgeführt ist

Um den Server bedingt neu zu starten, geben Sie als Root ein:

```
/sbin/service nfs condrestart
```

Um die NFS-Server-Konfigurationsdatei neu zu laden, ohne den Dienst neu zu starten, geben Sie als Root ein:

```
/sbin/service nfs reload
```

Standardmäßig startet der`nfs` Dienst *nicht* automatisch zum Zeitpunkt des Hochfahrens. Um das NFS so zu konfigurieren, dass es beim Hochfahren automatisch startet, verwenden Sie eine Initscript Utility, z.B. `/sbin/chkconfig`, **/sbin/ntsysv**, oder das **Services Configuration Tool** Programm. Siehe Kapitel *Controlling Access to Services* in *Red Hat Enterprise Linux Handbuch zur System-Administration* für weitere Informationen über diese Tools.

9.3. NFS-Server-Konfiguration

Es gibt drei Wege, einen NFS-Server unter Red Hat Enterprise Linux zu konfigurieren: die Verwendung von **NFS Server Configuration Tool** (`redhat-config-nfs`), die manuelle Veränderung der Konfigurationsdatei (`/etc/exports`), oder die Verwendung des `/usr/sbin/exportfs` Befehls.

Für Anweisungen bezüglich des **NFS Server Configuration Tool**, siehe Kapitel *Network File System (NFS)* im *Red Hat Enterprise Linux Handbuch zur System-Administration*. Der Rest dieses Abschnittes behandelt die manuelle Bearbeitung von `/etc/exports` und die Verwendung des `/usr/sbin/exportfs` Befehls für den Export von NFS-Dateisystemen.

9.3.1. NFS-Server-Konfigurationsdatei

Die Datei `/etc/exports` kontrolliert, welche Dateisysteme an Remote-Hosts exportiert werden und legt die Optionen fest. Leere Zeilen werden ignoriert, Kommentare können mithilfe des Rautezeichens `#` am Zeilenanfang eingegeben werden. Lange Zeilen können durch einen inversen Schrägstrich (`\`) umgebrochen werden. Jedes exportierte Dateisystem sollte eine eigene Zeile haben. Listen von autorisierten Hosts, die nach einem exportierten Dateisystem platziert sind, müssen durch Leerzeichen getrennt werden. Die Optionen für alle Hosts müssen in Klammern direkt nach der Hostbezeichnung stehen. Zwischen dem Host und der ersten Klammen darf kein Leerzeichen sein..

Eine Zeile für ein exportiertes Dateisystem hat die folgende Struktur:

```
<export> <host1>(<options>) <hostN>(<options>)...
```

Ersetzen Sie in dieser Struktur *<export>* mit dem Verzeichnis, das exportiert wird. Ersetzen Sie *<host1>* mit dem Host oder Netzwerk, mit dem der Export gemeinsam verwendet wird, und ersetzen Sie (*<options>* mit den Optionen für diesen Host oder dieses Netzwerk. Zusätzliche Hosts können in einer Liste durch Leerzeichen getrennt festgelegt werden.

Die folgende Methode kann dazu verwendet werden, Hostnamen festzulegen:

- *single host* — Ein bestimmter Host, einschließlich des kompletten Domain-Names, des Hostnamens oder der IP-Adresse wird festgelegt.
- *wildcards* — Dort, wo ein `*` oder ein `?` Zeichen verwendet werden, um eine Gruppierung von voll qualifizierten Domainnamen zu berücksichtigen, die mit einer bestimmten Reihe von Buchstaben übereinstimmen. Wildcards dürfen nicht mit IP-Adressen verwendet werden. Es kann aber mögliche sein, dass sie zufällig funktionieren, wenn die umgekehrten DNS- Lookups scheitern.

  Seien Sie jedoch beim Umgang mit Wildcards im Zusammenhang mit voll qualifizierten Domainnamen vorsichtig, da sie genauer arbeiten können als erwartet. So erlaubt die Verwendung von `*.example.com` als Wildcard zum Beispiel sales.example.com den Zugriff auf das exportierte Dateisystem, aber nicht bob.sales.example.com. Um beide Möglichkeiten zu erfassen, müssen sowohl `*.example.com` als auch `*.*.example.com` festgelegt werden.
- *IP networks* — Erlaubt die Übereinstimmung von Hosts auf der Basis ihrer IP-Adressen in einem großen Netzwerk. `192.168.0.0/28` lässt zum Beispiel die ersten 16 IP-Adressen von 192.168.0.0 bis 192.168.0.15 zu, um auf das exportierte Dateisystem zuzugreifen, aber nicht 192.168.0.16 und höher.
- *netgroups* — Lässt einen NIS-Netgroup-Namen zu, der wie folgt geschrieben wird: `@`*<group-name>*. Dadurch übernimmt der NIS-Server die Kontrolle für den Zugriff auf diese exportierten Dateisysteme, und Benutzer können ohne Auswirkung auf `/etc/exports` zu einer NFS- Gruppe hinzugefügt oder aus einer solchen entfernt werden.

`/etc/exports` benötigt in seiner einfachsten Form nur die Festlegung des Verzeichnisses, das exportiert wird, und den Host, der es verwenden kann. Z.B:

```
/exported/directory bob.example.com
```

In diesem Beispiel kann `bob.example.com` `/exported/directory/` mounten. Weil in diesem Beispiel keine Optionen festgelegt wurden, treten die folgenden NFS-Optionen in Kraft:

- `ro` — Schreibgeschützte Mounts des exportierten Dateisystems. Remote-Hosts können die Daten, die auf diesem Dateisystem gemeinsam verwendet werden, nicht verändern. Wenn Sie zulassen möchten, dass Hosts in dem Dateisystem Änderungen vornehmen, müssen Sie die Option `rw` verwenden (lesen und schreiben).
- `async` — Ermöglicht dem Server, in unregelmäßigen Abständen Daten auf die Platte zu schreiben. Diese Einstellung funktioniert am besten, wenn das exportierte Dateisystem schreibgeschützt ist. Wenn jedoch ein Host ein Dateisystem im beschreibbaren Modus ändert, können im Fall eines

Absturzes des Servers Daten verloren gehen. Mit der Option `sync` werden alle Dateien auf der Platte gesichert, bevor die Schreibanfrage des Clients vervollständigt wurde. Das kann allerdings die Leistung verlangsamen.

- `wdelay` — Weist den NFS-Server an, das Schreiben auf einer Platte zu verzögern, wenn das Aufheben des Schreibschutz-Modus bevorsteht. Dies kann die Leistung verbessern, indem die Anzahl der einzelnen Schreibbefehle für die Platte verringert wird. Mit der Option `no_wdelay` kann diese Funktion deaktiviert werden, die nur funktioniert, wenn Sie die Option `sync` verwenden.
- `root_squash` — Nimmt Root-Benutzern, welche von außen verbunden sind, deren Root-Rechte, indem diese die Benutzer-ID `nfsnobody` erhalten. Auf diese Weise wird die Kontrolle des Remote-Roots auf den niedrigsten lokalen Benutzer "gequetscht", was verhindert, dass Dateien auf dem Remote-Server unerlaubterweise verändert werden. Als Alternative können Sie mit der Option `no_root_squash` das "Sqashing" des Roots deaktivieren. Um jeden Remote-Benutzer, einschließlich Root, zu quetschen, verwenden Sie die Option `all_squash`. Um die Benutzer- und Gruppen-IDs festzulegen, die mit Remote-Benutzern eines bestimmten Hosts verwendet werden sollen, benutzen Sie die Optionen `anonuid` und `anongid`. Auf diese Weise können Sie für Remote NFS-Benutzer ein spezielles Benutzer-Konto (`anonuid=`<*`uid-value`*>`,anongid=`<*`gid-value`*>`)` erstellen und gemeinsam verwenden, wobei <*`uid-value`*>die Benutzer-ID-Nummer und<*`gid-value`*> die die gruppen-ID-Nummer ist.

Wichtig

Standardmäßig werden *access control lists* (*ACLs*) von NFS unter Red Hat Enterprise Linux unterstützt. Um diese Funktion zu deaktivieren, legen Sie die `no_acl` Option fest, wenn Sie das Dateisystem exportieren. Mehr Informationen zu dieser Funktion finden Sie im Kapitel*Network File System (NFS)* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Jede standardmäßige Einstellung für jedes exportierte Dateisystem muss ausdrücklich überschrieben werden. Wenn z.B. die `rw` Option nicht festgelegt ist, dann wird das exportierte Dateisystem schreibgeschützt gemeinsam verwendet. Im Folgenden eine Beispielszeile von`/etc/exports`, die zwei Standardoptionen überschreibt:

```
/another/exported/directory 192.168.0.3(rw,sync)
```

In diesem Beispiel kann `192.168.0.3` `/another/exported/directory/` beschreibbar mounten und alle Übertragungen auf die Platte werden auf der Platte gesichert, bevor die Schreibanfrage des Client abgeschlossen wird.

Wo keine Standardwerte angegeben sind, stehen zusätzliche Optionen zur Verfügung. Diese bieten die Möglichkeit, das Überprüfen der Sub-Trees zu deaktivieren, erlauben den Zugriff von unsicheren Ports sowie das Sperren unsicherer Dateien (für bestimmte frühere NFS-Client-Implementierungen notwendig). Auf der `exports`-man-Seite finden Sie weitere Details über diese weniger verwendeten Optionen.

Warnung

Das Format der Datei `/etc/exports` ist sehr präzisegestaltet, besonders im Bezug auf Leerzeichen. Denken Sie daran, exportierte Dateisystem immer getrennt von Hosts aufzuführen und Hosts durch Leerzeichen voneinander trennen. Es sollten jedoch keine weiteren Leerzeichen in der Datei sein, es sei denn, sie werden in Kommentarzeilen verwendet.

So bedeuten zum Beispiel die folgenden beiden Zeilen nicht das gleiche:

```
/home bob.example.com(rw)
/home bob.example.com (rw)
```

Die erste Zeile erlaubt nur Benutzern von `bob.example.com` den Zugriff im beschreibbaren Modus auf das Verzeichnis `/home`. Die zweite Zeile erlaubt Benutzern von `bob.example.com`, das Verzeichnis im schreibgeschützten Modus zu mounten (der Standard), alle anderen können es im beschreibbaren Modus mounten.

Für genaue Anweisungen zur Konfiguration eines NFS-Servers durch Bearbeitung von `/etc/exports`, siehe Kapitel *Server Security* in der *Red Hat Enterprise Linux Handbuch zur System-Administration*.

9.3.2. Der `exportfs` Befehl

Jedes Dateisystem, das via NFS an Remote-Benutzer exportiert wird, sowie die Zugriffsrechte für diese Dateisysteme werden in der Datei `/etc/exports` abgelegt. Wenn der `nfs` Dienst startet, wird diese Datei mit dem `/usr/sbin/exportfs`Befehl geöffnet und gelesen. Dann werden die für Remote-Benutzer verfügbaren Dateien an `rpc.mountd` und `rpc.nfsd` weitergegeben.

Mit der manuellen Ausführung des Befehls `/usr/sbin/exportfs` wird dem Root-Benutzer gestattet, Verzeichnisse selektiv zu exportieren oder nicht zu exportieren, ohne den NFS-Dienst neu starten zu müssen. Wenn `usr/sbin/exportfs` die korrekten Optionen erhält, wird dasexportierte Dateisystem in `/var/lib/nfs/xtab` gespeichert. Da `rpc.mountd` sich für das Festlegen der Privilegien für den Zugriff auf ein Dateisystem auf die Datei `xtab` bezieht, werden Änderungen an der Liste der exportierten Dateisysteme sofort wirksam.

Bei der Verwendung des Befehls `/usr/sbin/exportfs` stehen folgende übliche Optionen zur Verfügung:

- `-r` — Alle in `/etc/exports` aufgelistete Verzeichnisse werden exportiert und in `/etc/lib/nfs/xtab` wird eine neue Exportliste erstellt. Durch diese Option wird die Exportliste einschließlich aller Änderungen, die in `/etc/exports` vorgenommen wurden, aktualisiert.
- `-a` — Alle Verzeichnisse werden exportiert oder nicht exportiert, je nachdem, welche anderen Optionen in `/usr/sbin/exportfs` gewählt wurden. Wenn keine anderen Optionen festgelegt wurden, exportiert `/usr/sbin/exportfs` alle in `/etc/exports`festgelegten Dateisysteme.
- `-o` *`file-systems`* — Ermöglicht dem Benutzer, Verzeichnisse zum Exportieren festzulegen, die nicht in `/etc/exports` aufgeführt sind. Ersetzen Sie *`file-systems`* mit den zusätzlichen Dateisystemen, die exportiert werden sollen. Diese Dateisysteme müssen auf dieselbe Weise formatiert werden, wie sie in `/etc/exports` angegeben sind. Siehe Abschnitt 9.3.1 für weitere Informationen über die `/etc/exports` Syntax. Diese Option wird oft verwendet, um exportierte Dateisysteme zu testen, bevor sie endgültig zu der Liste der zu exportierenden Dateisysteme hinzugefügt werden.
- `-i` — Ignoriert `/etc/exports`; nur die Optionen, die von der Befehlszeile aus eingegeben wurden, werden zum Definieren der exportierten Dateisysteme verwendet.
- `-u` — Hebt den Export aller gemeinsam verwendeter Verzeichnisse auf. Der Befehl `/usr/sbin/exportfs -ua` unterbricht die gemeinsame Verwendung von NFS-Dateien, während alle NFS-Daemone weiter arbeiten. Geben Sie den Befehl `exportfs -r` ein, um die gemeinsame Verwendung von NFS-Dateien wieder fortzusetzen.
- `-v` — Verbose Operation, bei der exportierte oder nicht exportierte Dateisysteme detaillierter angezeigt werden, wenn der Befehl `exportfs` ausgeführt wird.

Wenn für den Befehl `/usr/sbin/exportfs` keine Optionen eingegeben werden, wird eine Liste der aktuell exportierten Dateisysteme angezeigt.

Für weitere Informationen über den `/usr/sbin/exportfs` Befehlsiehe `exportfs` man-Seite.

9.4. NFS-Client-Konfigurationsdateien

Gemeinsame NFS-Dateien mit dem `mount` Befehl auf die Seite des Clients gemountet. Das Format des Befehls lautet:

```
mount -o <options> <host>:</remote/export> </local/directory>
```

Ersetzen Sie *<options>* mit einer Komma- Trennliste der Optionen für das NFS-Dateisystem (für Details siehe Abschnitt 9.4.3). Ersetzen Sie *<host>* mit dem Remote-Host, *</remote/export>* mit dem Remote-Verzeichnis, das gemountet wird, und ersetzen Sie *</local/directory>* mit dem lokalen Verzeichnis, in dem das Remote-Dateisystem gemountet werden soll.

Für weitere Details siehe `mount` man-Seite.

Wenn mit dem manuellen `mount` Befehl auf ein NFS-Share zugegriffen wird, muss das Dateisystem manuell wieder gemountet werden, nachdem das System neu gestartet wurde. Red Hat Enterprise Linux bietet zwei Methoden an, mit denen Remote- Dateisysteme automatisch beim Hochfahren gemountet werden können: the `/etc/fstab` Datei oder der `autofs` Dienst.

9.4.1. `/etc/fstab`

Auf die `/etc/fstab` Datei wird von dem `netfs` Dienst zum Zeitpunkt des Hochfahrens verwiesen. Zeilen, die auf NFS-Shares verweisen haben daher den gleichen Effekt, als würde man während des Hochfahrens einen manuellen `mount` Befehl eingeben.

Eine Zeile `/etc/fstab` zum Mounten eines NFS-Exports sieht wie folgendes Beispiel aus:

```
<server>:</remote/export> </local/directory> nfs <options> 0 0
```

Ersetzen Sie *<server>* mit dem Hostnamen, der IP-Adresse oder dem voll qualifizierten Domain-Namen des Servers, der das Dateisystem exportiert.

Ersetzen Sie *</remote/export>* mit dem Pfad zum exprotierten Verzeichnis.

Ersetzen Sie *</local/directory;>* mit dem lokalen Dateisystem, auf dem das exportierte Verzeichnis gemountet ist. Dieser Mount-Punkt muss vorhanden sein, bevor `/etc/fstab` gelesen wird oder das Mounten scheitert.

Die Option `nfs` gibt den Typ des gemounteten Dateisystems an.

Ersetzen Sie *<options>* mit einer Komma- Trennliste der Optionen für das NFS-Dateisystem. (Details siehe Abschnitt 9.4.3). Zusätzliche Informationen finden Sie auf der `fstab` man-Seite.

9.4.2. `autofs`

Ein Nachteil bei der Verwendung von `/etc/fstab` ist, dass das System Ressourcen zur Verfügung stellen muss, ungeachtet dessen, wie wenig das gemountete Dateisystem verwendet wird. Nur so verbleibt es an dieser Stelle. Bei einem oder zwei Mounts ist das kein Problem, wenn Ihr System jedoch zur gleichen Zeit Mounts von Dutzenden Systemen warten muß, kann die Leistungsfähigkeit des Systems darunter leiden. Eine Alternative zu `/etc/fstab` ist die Verwendung des auf dem Kernel basierenden Dienstprogramms `automount`, das NFS-Dateisysteme automatisch mountet und unmountet und dabei Ressourcen einspart..

Der `autofs` Dienstwird dazu verwendet, den`automount`Befehl über die primäre Konfigurationsdatei `/etc/auto.master` zu steuern. Zwar kann `automount` in der Befehlszeile festgelegt werden, es ist aber bequemer, die Mount-Punkte, den Hostnamen, das exportierte Verzeichnis und die Optionen mit einer Gruppe von Dateien festzulegen, als sie manuell eingeben zu müssen.

Die Konfigurationsdateien `autofs` sind in einem über- bzw. untergeordneten Verhältnis festgelegt. Die wichtigste Konfigurationsdatei (`/etc/auto.master`) führt Mount-Punkte in Ihrem System an,

die mit einem bestimmten *Zuordnungstyp* verbunden sind, der die Form von anderen Konfigurationsdateien, Programmen, NIS-Maps oder anderen weniger bekannte Methoden zum Mounten annehmen kann. Die Datei `auto.master` enthält Zeilen, die auf diese Mount-Punkte verweisen und wie folgt aussehen:

```
<mount-point> <map-type>
```

Das <*Mount-Punkt*> Element zeigt den Ort des Mount in dem lokalen Dateisystem an. Der <*Zuordnungstyp*> bezieht sich auf die Art, wie der Mount-Punkt gemountet wird. Üblicherweise wird zum automatischen Mounten von NFS-Exporten eine Datei als Zuordnungstyp für einen bestimmten Mount-Punkt verwendet. Die Zuordnungsdatei wird normalerweise wie folgt bezeichnet: `auto.`<*Mount-Punkt*>, wobei <*Mount-Punkt*> der in `auto.master` bezeichnete Mount-Punkt ist. Eine Zeile in den Zuordnungsdateien zum Mounten einens NFS-Exports sieht wie folgendes Beispiel aus:

```
</local/directory>  -<options>  <server>:</remote/export>
```

Ersetzen Sie <*/local/directory;*> mit dem lokalen Dateisystem, auf dem das exportierte Verzeichnis gemountet wird. Dieser Mount-Punkt muss existieren, bevor die Zuordnungsdatei gelesen wird, sonst scheitert der Mount.

Ersetzen Sie <*options*> mit einer Komma- Trennliste mit den Optionen für das NFS-Dateisystem. (Für Details siehe Abschnitt 9.4.3). Stellen sie sicher, dass Sie das Bindestrich-Zeichen (`-`) unmittelbar vor der Optionsliste eingeben.

Ersetzen Sie <*server*> mit dem Hostnamen, der IP-Adresse oder dem voll qualifizierten Domain-Namen des Servers, der das Dateisystem exportiert.

Ersetzen Sie <*/remote/export*> mit dem Pfad zum exprotierten Verzeichnis.

Ersetzen Sie <*options*> mit einer Komma- Trennliste für die Optionen des NFS-Dateisystems. (Für Details siehe Abschnitt 9.4.3).

Da die `autofs`-Konfigurationsdateien für eine Anzahl verschiedener Mounts für viele Arten von Geräten und Dateisystemen verwendet werden können, sind sie besonders für die Erstellung von NFS-Mount hilfreich. Einige Organisationen speichern zum Beispiel das Benutzerverzeichnis `/home/` mithilfe eines NFS-Shares auf einem zentralen Server. Anschließend wird die Datei `auto.master` auf jeder Workstation konfiguriert, um auf eine `auto.home`-Datei zu verweisen, die genaue Angaben enthalten, wie das Verzeichnis `/home/` via NFS zu mounten ist. Der Benutzer erhält soZugriff auf persönliche Daten und Konfigurationsdateien im Verzeichnis `/home/`, indem er sich irgendwo im internen Netzwerk anmeldet. In diesem Fall würde die Datei `auto.master` wie folgt aussehen:

```
/home    /etc/auto.home
```

Dies stellt den `/home/`-Mount-Punkt auf dem lokalen System so ein, dass er mit der Datei `/etc/auto.home` konfiguriert wird, die wie folgendes Beispiel aussieht:

```
*  -fstype=nfs,soft,intr,rsize=8192,wsize=8192,nosuid,tcp  server.example.com:/home
```

Diese Zeile gibt an, dass jeder Versuch eines Benutzers, im lokalen `/home/`-Verzeichnis (aufgrund des Sternchens) auf irgendein Verzeichnis zuzugreifen, einen NFS-Mount auf dem `server.example.com`-System innerhalb des exportierten Dateisystems zur Folge hat. Die Mount-Optionen geben an, dass bei jedem NFS-Mount des `/home/` -Verzeichnisses bestimmte Einstellungen verwendet werden. Weitere Informationen über Mount-Optionen, einschließlich der in diesem Beispiel verwendeten, finden Sie unter Abschnitt 9.4.3.

Für weitere Informationen über `autofs` Konfigurationsdateien siehe die `auto.master` man-Seite.

9.4.3. Allgemeine NFS-Mount-Optionen

Neben dem Mounten eines Dateisystems auf einem Remote-Host via NFS können eine Anzahl anderer Optionen zum Zeitpunkt des Mountens festgelegt werden. Diese Optionen können gemeinsam mit den manuellen `mount`-Befehlen, `/etc/fstab`- Einstellungen und`autofs` verwendet werden.

Im Folgenden sind die üblichen Optionen für NFS-Mounts aufgeführt:

- `hard` oder `soft` — Legt fest, ob das Programm, das eine Datei über eine NFS-Verbindung verwendet, anhalten und auf den Server warten soll (`hard`), bis dieser wieder online ist, wenn der Host, der das exportierte Dateisystem betreut, nicht zur Verfügung steht oder einen Fehler meldet (`soft`).

  Wenn Sie `hard` festlegen, können Sie den Prozess des Wartens auf eine NFS-Verbindung nicht aufheben, es sei denn, Sie haben auch die Option `intr` festgelegt.

  Wenn Sie die Option `soft` bestimmen, können Sie eine weitere `timeo=`<*Wert*> Option einstellen, wobei <*Wert*> die Zeit (in Sekunden) festlegt, die vergeht, bevor ein Fehler gemeldet wird.
- `intr` — Ermöglicht, dass die NFS-Anfragen unterbrochen werden können, wenn der Server ausfällt oder nicht erreicht werden kann.
- `nfsvers=2` oder `nfsvers=3` — Legt fest, welche Version des NFS-Protokolls verwendet werden soll.
- `nolock` — Deaktiviert das Sperren von Dateien. Diese Einstellung wird gelegentlich für die Verbindung zu einem alten NFS-Server benötigt.
- `noexec` — Verhindert das Ausführen von Binärdateien auf dem gemounteten Dateisystem. Diese Option ist hilfreich, wenn Ihr System ein Nicht-Linux Dateisystem über NFS mountet, das inkompatible Binärdateien enthält.
- `nosuid` — Deaktiviert Set-User-Identifier oder Set-Group- Identifier-Bits. Diese Funktion verhindert, dass Remote-Benutzer höhere Privilegien erlangen, indem sie ein Setuid-Programm ausführen.
- `rsize=8192` und `wsize=8192` — Können NFS-Kommunikationen zum Lesen (`rsize`) und Schreiben (`wsize`) beschleunigen, indem das Ausmaß des Datenblocks (in Bytes) vergrößert wird, der übertragen wird. Beim Ändern dieser Werte sollten Sie beachten, dass einige ältere Linux-Kernel und Netzwerkkarten eventuell mit einem größeren Datenblock nicht korrekt arbeiten.
- `tcp` — Legt für den NFS-Mount die Verwendung des TCP- Protokolls anstatt von UDP fest.

Auf der `mount`-man-Seite stehen noch viele weitere Optionen zur Verfügung, einschließlich Optionen, die beim Mounten eines Nicht-NFS-Dateisystems verwendet werden.

9.5. NFS Sichern

Die Art, wie NFS bei der gemeinsamen Verwendung ganzer Dateisysteme mit einer großen Anzahl bekannter Hosts arbeitet, ist gut zu durchschauen. Aus diesem Vorteil können sich jedoch auch eine Reihe potenzieller Sicherheitsprobleme ergeben.

Folgende Punkte sollten beim Exportieren von NFS-Dateisystemen auf einem Server oder beim Mounten auf einem Client beachtet werden. Dadurch können die Sicherheitsrisiken von NFS verringert und die Daten auf dem Server besser geschützt werden.

Eine kurze Auflistung von Schritten, die Administratoren zur Sicherung von NFS ausführen können, lesen Sie das Kapitel *Server Security* in der *Red Hat Enterprise Linux Sicherheitshandbuch*.

9.5.1. Host-Zugriff

NFS steuert anhand des Hosts, der die Anfrage zum Mounten stellt, wer ein exportiertes Dateisystem mounten kann (und nicht anhand des Benutzers, der das Dateisystem tatsächlich verwendet). Die Hosts müssen über eine ausdrücklicheBerechtigung verfügen, exportierte Dateisysteme zu mounten. Für Benutzer ist keine Zugriffskontrolle möglich, mit Ausnahme der Berechtigungen für Dateien und Verzeichnisse. Mit anderen Worten, wenn ein Dateisystem via NFS exportiert wird, kann jeder Benutzer auf jedem Remote-Host, der mit dem NFS-Server verbunden ist, auf die gemeinsam verwendeten Daten zugreifen. Um die potentiellen Risiken zu limitieren, erlauben Administratoren oft nur schreibgeschützten Zugang oder quetschen Benutzer- Genehmigungen zu einer üblichen Benutzer- und Gruppen-ID zusammen. Leider verhindern diese Lösungen, dass das NFS-Share so genützt wird, wie ursprünglich beabsichtigt.

Wenn ein Angreifer die Kontrolle über den DNS-Server erlangt, der vom System zum Exportieren des NFS-Dateisystems verwendet wird, kann das System, dem ein bestimmter Hostname oder der komplette Domain-Name zugeordnet ist, auf einen nicht autorisierten Computer hinweisen. An diesem Punkt *ist* dieser nicht autorisierte Computer das System, das das NFS-Share mounten kann, da keine Informationen über Benutzernamen oder Passwort ausgetauscht werden, um zusätzliche Sicherheit für den NFS-Mount zu garantieren.

Wildcards sollten sparsam verwendet werden, wenn Verzeichnisse über NFS exportiert werden, da sich der Wirkungsbereich der Wildcard mehr Systeme als gewollt ausdehnen kann.

Es ist auch möglich, den Zugang zum `portmap` Dienstmittels TCP-Wrapper einzuschränken. Der Zugang zu Ports, die `portmap`, `rpc.mountd`, und `rpc.nfsd` verwenden, kann ebenfalls eingeschränkt werden, indem mit `iptables` Firewall-Regeln aufgestellt werden.

Für weitere Informationen über das Sichern von NFS `portmap` siehe Kapitel *Server Security* in der *Red Hat Enterprise Linux Sicherheitshandbuch*. Zusätzliche Informationen über Firewalls finden Sie in Kapitel 15.

9.5.2. Dateiberechtigungen

Wenn ein Remote-Host das NFS-Dateisystem im Read-Write-Modus gemountet hat, sind die Genehmigungen der einzige Schutz, den jede gemeinsame Datei hat.Zwei Benutzer, die die gleiche Benutzer-ID zum Mounten des gleichen NFS-Dateisystems verwenden, können ihre Dateien gegenseitig modifizieren. Jeder, der als Root angemeldet ist, kann den Befehl `su -` verwenden, um ein Benutzer zu werden und über das NFS-Share Zugang zu bestimmten Dateien zu erlangen. Mehr Information über Konflikte zwischen NSF und Benutzer-ID finden Sie im Kapitel*Managing User Accounts and Resource Access* im *Red Hat Enterprise Linux Introduction to System Administration*.

Standardmäßig werden Zugangs-Unterstützungslisten (ACLs) von NFS unter Red Hat Enterprise Linux unterstützt. Es wird nicht empfohlen, diese Funktion zu deaktivieren. Mehr dazu finden Sie im Kapitel *Network File System (NFS)* in der *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Standardmäßig wird beim Exportieren eines Dateisystems via NFS *Root-Squashing* verwendet. Dies setzt die Benutzer-ID von jedem, der auf die NFS-Share zugreift, auf dem jeweiligen lokalen Rechner auf einen Wert des `nfsnobody`-Accounts auf dem Server. Schalten Sie Root-Squashing niemals aus.

Wenn Sie eine NFS-Share als schreibgeschützt exportieren, verwenden Sie die Option `all_squash`, wodurch alle Benutzer, die auf Ihr exportiertes Dateisystem Zugriff haben, die Benutzer-ID `nfsnobody` erhalten.

9.6. Zusätzliche Informationsquellen

Das Verwalten eines NFS-Servers kann eine Herausforderung sein. Es gibt viele Optionen, um NFS-Dateisysteme zu exportieren oder zu mounten. Einige davon wurden in diesem Kapitel nicht erwähnt. Weitere Informationen finden Sie in den angegebenen Quellen.

9.6.1. Installierte Dokumentation

- `/usr/share/doc/nfs-utils-<Versionsnummer>/` — Ersetzen Sie `<Versionsnummer>` mit der Versionsnummer des installierten NFS Pakets. Dieses Verzeichnis enthält einen Menge an Informationen über die NFS-Implementierung für Linux, wobei auch ein Blick auf die verschiedenen NFS-Konfigurationen und ihre Auswirkungen auf die Übertragung von Dateien geworfen wird.
- `man mount` — Enthält einen umfassenden Überblick über die Mount-Optionen für NFS Server- und Client-Konfigurationen.
- `man fstab` — Bietet Details über das Format der Datei `/etc/fstab`, die beim Hochfahren des Systems Dateisysteme mountet.
- `man nfs` — Liefert Details über den Export von NFS-spezifischen Dateisystemen und Mount-Optionen.
- `man exports` — Zeigt allgemeine Optionen an, die während des Exportierens von NFS-Dateisystemenin der Datei `/etc/exports` verwendet werden.

9.6.2. Nützliche Websites

- http://sourceforge.net/projects/nfs/ — Die Homepage des Linux NFS Project und eine großartige Quelle für Projektstatus-Upgrades.

9.6.3. Zusätzliche Literatur

- *Managing NFS and NIS* von Hal Stern, Mike Eisler und Ricardo Labiaga; O'Reilly & Associates — Ein hervorragendes Referenzhandbuch für die vielen verschiedenen NFS-Exporte und die zur Verfügung stehenden Mount-Optionen.
- *NFS Illustrated* von Brent Callaghan; Addison-Wesley Publishing Company — Vergleicht NFS mit anderen Netzwerk-Dateisystemen und zeigt, wie die NFS- Kommunikation zustande kommt.
- *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Das Kapitel *Network File System (NFS)* erklärt in knapper Weise, wie NFS-Clients und Server erstellt werden.
- *Red Hat Enterprise Linux Sicherheitshandbuch*; Red Hat, Inc. — Das Kapitel *Server Security* erläutert Wege zur Sicherung von NFS und anderer Dienste.

redhat

Kapitel 10.

Apache HTTP Server

Apache HTTP Server ist ein robuster und kommerzieller Open Source Web-Server, der von der Apache Software Foundation (http://www.apache.org) entwickelt wurde. Red Hat Enterprise Linux enthät die Apache HTTP Server Version 2.0 sowie eine Reihe von Server-Modulen, die seine Funktionalität erweitern.

Die mit Apache HTTP Server installierte Standardkonfigurationsdatei ist in den meisten Situationen unverändert einsetzbar. Dieses Kapitel zeigt, wie die Apache HTTP Server Konfigurationsdatei (`/etc/httpd/conf/httpd.conf`) für Situationen angepasst werden kann, in denen die Standardkonfiguration nicht Ihren Anforderungen genügt, oder Sie eine Konfigurationsdatei vom älteren Apache HTTP Server 1.3 Format konvertieren müssen.

Warnung

Wenn Sie vorhaben, das graphische **HTTP Configuration Tool** (`redhat-config-httpd`) zu verwenden, editieren Sie *nicht* die Apache HTTP Server Konfigurationsdatei. Das **HTTP Configuration Tool** erstellt diese Datei jedes Mal neu, wenn sie verwendet wird.

Weitere Informationen zum **HTTP Configuration Tool** finden Sie im Kapitel *Apache HTTP Server-Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

10.1. Apache HTTP Server 2.0

Es gibt einige wichtige Unterschiede zwischen Apache HTTP Server Version 2.0 und Version 1.3 (die mit der Release Red Hat Linux 7.3 und früher ausgeliefert wurde). Dieser Abschnitt gibt einen Überblick über einige der neuen Merkmale von Apache HTTP Server 2.0 und weist auf wichtige Änderungen hin. Möchten Sie eine Konfigurationsdatei der Version 1.3. in das neue Format migrieren, lesen Sie Abschnitt 10.2.

10.1.1. Merkmale von Apache HTTP Server 2.0

Die Einführung von Apache HTTP Server 2.0 bringt eine Reihe neuer Merkmale mit sich. Einige davon sind:

- *Neue Apache API* — Apache HTTP Server hat eine Reihe neuer, besserer Application Programing Interfaces (APIs) für Module.

  Wichtig

  Für Apache HTTP Server 1.3 gebaute Module funktionieren nicht, wenn diese nicht auf die neue API angepasst wurden. Wenn Sie sich nicht sicher sind, ob ein bestimmtes Modul angepasst wurde oder nicht, wenden Sie sich an die für die Paket-Pflege zuständige Stelle *bevor* Sie aktualisieren.

- *Filtern* — Module für Apache HTTP Server 2.0 sind in der Lage, Inhalte zu filtern. Weitere Informationen dazu finden Sie unter Abschnitt 10.2.4.
- *IPv6 Support* — Apache HTTP Server 2.0 unterstützt die IP-Adressfunktionen der nächsten Generation.

- *Vereinfachte Anweisungen* — Eine Reihe verwirrender Anweisungen wurden entfernt und andere vereinfacht. Informationen zu speziellen Anweisungen finden Sie unter Abschnitt 10.5.
- *Mehrsprachige Fehlermeldungen* — Bei der Verwendung von *Server Side Include* (*SSI*) Dokumenten, können beutzerdefinierbare Seiten zu Fehlermeldungen in mehreren Sprachen verschickt werden.
- *Mehrfach-Protokoll-Support* — Apache HTTP Server 2.0 kann mehrere Protokolle unterstützen.

Eine vollständigerere Liste der Änderungen finden Sie online unter http://httpd.apache.org/docs-2.0/.

10.1.2. Packetänderungen bei Apache HTTP Server 2.0

In Red Hat Linux 9 wurde das Apache HTTP Server-Paket umbenannt. Außerdem wurden einige verwandte Pakete umbenannt, verworfen oder in andere Pakete aufgenommen.

Es folgt eine Liste der Paketänderungen:

- Die `apache`, `apache-devel` und `apache-manual` Pakete wurden jeweils umbenannt in `httpd`, `httpd-devel` und `httpd-manual`.
- Das Paket `httpd` enthält jetzt `mod_dav`.
- Die Pakete `mod_put` und `mod_roaming` wurden herausgenommen, da deren Funktionen bereits in `mod_dav` enthalten sind.
- Die Pakete `mod_auth_any` und `mod_bandwidth` wurden herausgenommen.
- Die Versionsnummer für das Paket `mod_ssl` wurde jetzt mit dem Paket `httpd` in Einklang gebracht. Dies bedeutet, dass das Paket `mod_ssl` für Apache HTTP Server 2.0 eine *niedrigere* Versionsnummer hat als das Paket `mod_ssl` für Apache HTTP Server 1.3.

10.1.3. Dateisystemänderungen bei Apache HTTP Server 2.0

Bei der Aktualisierung auf Apache HTTP Server 2.0 ergeben sich folgende Änderungen am Layout des Dateisystems:

- *Ein neues Konfigurationsverzeichnis `/etc/httpd/conf.d/` wurde hinzugefügt.* — Dieses neue Verzeichnis wird zur Hinterlegung von Konfigurationsdateien für Module in Einelpakete verwendet wie `mod_ssl`, `mod_perl` und `php`. Der Server wird angewiesen, anhand der Anweisung `Include conf.d/*.conf` in der Apache HTTP Server Konfigurationsdatei `/etc/httpd/conf/httpd.conf` Konfigurationsdateien aus diesem Speicherplatz zu laden.

  Wichtig

  Es ist sehr wichtig, dass die Zeile für das neue Konfigurationsverzeichnis beim Migrieren einer bestehenden Konfiguration eingefügt wird.

- *Die Programme `ab` und `logresolve` wurden verschoben.* — Diese Dienstprogramme wurden vom Verzeichnis `/usr/sbin/` in das Verzeichnis `/usr/bin/` umgelagert. Dies hat zur Folge, dass Skripts mit absoluten Pfaden für diese Binärdateien scheitern.
- *Der Befehl `dbmmanage` wurde ersetzt.* — Der Befehl `dbmmanage` wurde durch `htdbm` ersetzt. Weitere Informationen erhalten Sie unter Abschnitt 10.2.4.4.
- *Die Konfigurationsdatei `logrotate` wurde umbenannt.* — Die Konfigurationsdatei `logrotate` wurde von `/etc/logrotate.d/apache` umbenannt in `/etc/logrotate.d/httpd`.

Der nächste Abschnitt zeigt, wie eine Apache HTTP Server 1.3 Konfiguration in das neue Format 2.0 migriert werden kann.

10.2. Migrieren von Apache HTTP Server 1.3 Konfigurationsdateien

Der nächste Abschnitt zeigt, wie eine Apache HTTP Server 1.3 Konfiguration in das neue Format von Apache HTTP Server 2.0 migriert werden kann.

Wenn Ihr Server von Red Hat Enterprise Linux 2.1 auf Red Hat Enterprise Linux 3 aktualisiert wurde, und Apache HTTP Server bereits installiert war, dann wird die neue Stock-Konfigurationsdatei für das Apache HTTP Server 2.0-Paket als `/etc/httpd/conf/httpd.conf.rpmnew` installiert und Ihre Originalversion 1.3 `httpd.conf` beibehalten. Es liegt natürlich ganz bei Ihnen, ob Sie die neue Konfigurationsdatei verwenden möchten und Ihre alten Einstellungen dorthin migrieren oder die vorhandene Datei als Basis verwenden und sie entsprechend anpassen; einige Bereiche der Datei haben sich jedoch mehr als andere verändert, deshalb ist ein gemischtes Vorgehen normalerweise die beste Lösung. Die Stock-Konfigurationsdateien sowohl für Version 1.3 als auch für Version 2.0 werden in drei Abschnitte unterteilt. Ziel dieses Leitfadens ist es, den hoffentlich einfachsten Weg aufzuzeigen.

Handelt es sich bei `/etc/httpd/conf/httpd.conf` um eine modifizierte Version der Standard Red Hat-Version und Sie haben eine Kopie des Originals gespeichert, dann ist es vielleicht am einfachsten, wenn Sie den Befehl `diff` aufrufen, wie in folgendem Beispiel gezeigt:

```
diff -u httpd.conf.orig httpd.conf | less
```

Dieser Befehl hebt die von Ihnen durchgeführten Änderungen hervor. Besitzen Sie keine Kopie der Originaldatei, entnehmen Sie sie anhand der Befehle `rpm2cpio` und `cpio` einem RPM-Paket, wie in folgendem Beispiel gezeigt:

```
rpm2cpio apache-<version-number>.i386.rpm | cpio -i --make
```

In the above command, replace *<version-number>* with the version number for the `apache` package.

Es ist hilfreich zu wissen, dass Apache HTTP Server über einen Testmodus zur Prüfung Ihrer Konfigurations auf Fehler verfügt. Der Zugriff erfolgt über folgenden Befehl:

```
apachectl configtest
```

10.2.1. Globale Umgebungskonfiguration

Der globale Umgebungsabschnitt der Konfigurationsdatei enthält Anweisungen, die sich insgesamt auf die Funktionsweise von Apache HTTP Server auswirken, wie die Anzahl konkurrierender Anfragen, die abgefertigt werden und die Speicherplätze der verschiedenen verwendeten Dateien. Bei diesem Abschnitt ist im Vergleich zu den anderen eine große Anzahl an Änderungen notwendig. Es empfiehlt sich deshalb, dass dieser Abschnitt seine Basis in der Apache HTTP Server 2.0 Konfigurationsdatei hat und Sie Ihre alten Einstellungen dorthin migrieren.

10.2.1.1. Interface- und Port-Binding

Die Anweisungen `BindAddress` und `Port` existieren nicht mehr; ihre Funktionen wurde durch eine flexiblere `Listen` Anweisung ersetzt.

Wenn Sie in Ihrer 1.3. Version die Konfigurationsdatei auf `Port 80` gesetzt haben, sollten Sie diese auf `Listen 80` umändern. Hatten Sie `Port` auf einen Wert gesetzt, *der nicht 80 war* dann müssen Sie auch die Port-Nummer an den Inhalt Ihrer `ServerName` Anweisung anhängen.

Folgendes ist ein Beispiel einer Apache HTTP Server 1.3 Anweisung:

```
Port 123
ServerName www.example.com
```

Verwenden Sie folgende Struktur um diese Einstellung zu Apache HTTP Server 2.0 zu migrieren:

```
Listen 123
ServerName www.example.com:123
```

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- `http://httpd.apache.org/docs-2.0/mod/mpm_common.html#listen`
- `http://httpd.apache.org/docs-2.0/mod/core.html#servername`

10.2.1.2. Server-Pool Größeneinstellung

Wenn Apache HTTP Server Anforderungen annimmt, werden Child-Prozesse oder Threads erzeugt, die diese übernehmen. Diese Gruppe von Child-Prozessen oder Threads wird *server-pool* genannt. Die Verantwortung der Handhabung von Annahmen und Versenden von Child-Prozessen wurde in Apache HTTP Server 2.0 in einer Modulgruppe mit dem Namen *Multi-Processing Modules* (*MPMs*)zusammengefasst. Im Gegensatz zu anderen Modulen kann nur ein Modul der MPM-Gruppe von Apache HTTP Server geladen werden, da ein MPM-Modul für grundlegende Anfragebearbeitung und -verteilung zuständig ist. Drei MPM-Module werden mit der Version 2.0 ausgeliefert: `prefork`, `worker`, and `perchild`. Lediglich `prefork` und `worker` MPMs sind zur Zeit verfügbar, das `perchild` MPM könnte allerdings zu einem späteren Zeitpunkt verfügbar werden.

Das standardmäßige Verhalten des Apache HTTP Server 1.3 wurde in das `prefork` MPM verlagert. Das `prefork` MPM akzeptiert die gleichen Anweisungen wie Apache HTTP Server 1.3. Folgende Anweisungen können direkt migriert werden:

- `StartServers`
- `MinSpareServers`
- `MaxSpareServers`
- `MaxClients`
- `MaxRequestsPerChild`

Das `worker` MPM implementiert einen Multi-Process, Multi-Threaded Server, der eine größere Skalierbarkeit bietet. Wenn dieses MPM verwendet wird, werden Anfragen durch Threads gehandhabt, was Systemreserven spart und es einer größeren Anzahl von Anfragen erlaubt effizient beantwortet zu werden. Obwohl einige der von der `worker` MPM akzeptierten Anweisungen die selben sind wie die von der `prefork` MPM akzeptierten, sollten die Werte nicht direkt von einer Apache HTTP Server 1.3 Installation übertragen werden. Es ist am Besten, die Standardwerte als Richtlinie zu nehmen, und dann zu Experimentieren, um die geeignetsten Werte zu bestimmen.

Wichtig

Um das `worker` MPM zu verwenden, erzeugen Sie die Datei `/etc/sysconfig/httpd`. Fügen Sie folgende Anweisungen zu der Datei hinzu:

```
HTTPD=/usr/sbin/httpd.worker
```

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mpm.html

10.2.1.3. Support für Dynamic Shared Objects (DSO)

Viele Änderungen sind hier notwendig und es empfiehlt sich für jeden, der versucht, eine Apache HTTP Server 1.3-Konfiguration an eine 2.0-Konfiguration anzupassen (im Gegensatz zur Migration Ihrer Änderungen in die 2.0-Konfiguration), diesen Abschnitt aus der Apache HTTP Server 2.0 Stock-Konfigurationsdatei zu kopieren.

Diejenigen, die den Abschnitt immer noch nicht aus der Stock - Apache HTTP Server 2.0-Konfiguration kopieren möchten, sollten Folgendes beachten:

- Die Anweisungen `AddModule` und `ClearModuleList` existieren nicht mehr. Diese Anweisungen wurden verwendet, um sicherzustellen, dass Module in der richtigen Reihenfolge aktiviert werden konnten. Apache 2.0 API erlaubt es den Modulen, ihre Reihenfolge anzugeben, womit diese beiden Anweisungen überflüssig werden.
- Die Reihenfolge der `LoadModule` Zeilen ist nicht mehr von Bedeutung.
- Viele Module wurden hinzugefügt, entfernt, umbenannt, aufgeteilt oder zusammengefasst.
- `LoadModule` Zeilen für Module, die in ihren eigenen RPMs (`mod_ssl`, `php`, `mod_perl` und ähnliche) verpackt sind, sind nicht mehr notwendig, da sie sich in der entsprechenden Datei im `/etc/httpd/conf.d/` Verzeichnis befinden.
- Die verschiedenen `HAVE_XXX` Definitionen werden nicht mehr festgelegt.

Wichtig

Sollten Sie versuchen, Ihre Originaldatei zu ändern, beachten Sie bitte, dass es äußerst wichtig ist, dass Ihre `httpd.conf` folgende Anweisung enthält:

```
Include conf.d/*.conf
```

Das Weglassen dieser Anweisung hat zur Folge, dass alle Module scheitern, die in ihren eigenen RPMs (wie `mod_perl`, `php` und `mod_ssl`) verpackt sind.

10.2.1.4. Sonstige globale Umgebungsänderungen

Folgende Anweisungen wurden aus der Apache HTTP Server 2.0 Konfiguration entfernt:

- *`ServerType`* — Der Apache HTTP Server kann nur als `ServerType standalone` gestartet werden, womit diese Anweisung keine Bedeutung mehr hat.
- *`AccessConfig`* und *`ResourceConfig`* — Diese Anweisungen wurden herausgenommen, da sie die gleiche Funktion wie die `Include` Anweisung haben. Haben Sie `AccessConfig` und `ResourceConfig` Anweisungen gesetzt, dann müssen sie diese durch `Include` Anweisungen ersetzen.

  Um sicherzustellen, dass die Dateien in der Reihenfolge gelesen werden, die von den älteren Anweisungen vorgesehen war, sollten Sie `Include` Anweisungen an das Ende von `httpd.conf` setzen.

Dabei sollte die Anweisung, die `ResourceConfig` entspricht, vor der Anweisung liegen, die `AccessConfig` entspricht. Haben Sie mit Standardwerten gearbeitet, müssen Sie diese ausdrücklich als `conf/srm.conf` und `conf/access.conf` mit aufnehmen.

10.2.2. Hauptserver-Konfiguration

Der Abschnitt zur Hauptserver-Konfiguration der Konfigurationsdatei richtet den Hauptserver ein, der auf alle Anfragen antwortet, die nicht über eine <`VirtualHost`> Definition gehandhabt werden. Die Werte hier liefern auch Standardwerte für alle <`VirtualHost`> Definitionen, die Sie eventuell definieren möchten.

In den Anweisungen dieses Abschnitts gibt es kaum Unterschiede zwischen Apache HTTP Server 1.3 und Version 2.0. Wenn Ihre Hauptserver-Konfiguration sehr stark benutzerdefiniert ist, ist es vielleicht einfacher für Sie, wenn Sie Ihre bereits existierende Konfiguration an Apache HTTP Server 2.0 anpassen. Benutzer mit weniger benutzerdefinierten Hauptserver-Abschnitten sollten ihre Änderungen in die Apache HTTP Server 2.0 Stock-Konfiguration migrieren.

10.2.2.1. `UserDir` Mapping

Die Anweisung `UserDir` wird verwendet um URLs wie `http://example.com/~bob/` in ein Unterverzeichnis innerhalb des Home-Verzeichnisses des Benutzers `bob` wie `/home/bob/public_html` abzubilden. Als Nebenwirkung erlaubt es diese Eigenschaft einem potentiellen Unbefugten festzustellen, ob ein bestimmter Benutzername im System vorhanden ist. Aus diesem Grund ist diese Anweisung in der Standardkonfiguration von Apache HTTP Server 2.0 deaktiviert.

Aktivieren Sie die `UserDir` Abbildung durch Umändern der sich in `httpd.conf` befindlichen Anweisung von:

```
UserDir disable
```

in folgende:

```
UserDir public_html
```

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_userdir.html#userdir

10.2.2.2. Logging

Folgende Log-Anweisungen wurden entfernt:

- `AgentLog`
- `RefererLog`
- `RefererIgnore`

Agent- und Referrer-Logs sind über `CustomLog` und `LogFormat` Anweisungen immer noch verfügbar.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#customlog
- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#logformat

10.2.2.3. Index-Erstellung für Verzeichnisse

Die veraltete Anweisung`FancyIndexing` wurde entfernt. Die gleiche Funktionalität ist über `FancyIndexing` *Option* in der Anweisung `IndexOptions` verfügbar.

Die neue Option `VersionSort` für die `IndexOptions` Anweisung führt dazu, dass Dateien mit Versionsnummern auf natürliche Weise sortiert werden, so dass `httpd-2.0.6.tar` in einer Verzeichnis-Indexseite vor `httpd-2.0.36.tar` erscheinen würde.

Die Standardwerte für die Anweisungen `ReadmeName` und `HeaderName` haben sich geändert, und zwar von `README` und `HEADER` in `README.html` und `HEADER.html`.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#indexoptions
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#readmename
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#headername

10.2.2.4. Inhaltsverhandlung

Die Anweisung `CacheNegotiatedDocs` kann jetzt die Argumente `on` oder `off` haben. Existierende Fälle von `CacheNegotiatedDocs` sollten durch `CacheNegotiatedDocs on` ersetzt werden.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_negotiation.html#cachenegotiateddocs

10.2.2.5. Fehlerdokumente

Um eine feste Meldung mit der `ErrorDocument` Anweisung zu verwenden, sollte die Meldung von einem Paar doppelter Anführungszeichen umschlossen sein, anstatt dass nur doppelte Anführungszeichen der Meldung vorangestellt werden, wie in Apache 1.3. verlangt.

Folgendes ist ein Beispiel einer Apache HTTP Server 1.3 Anweisung:

```
ErrorDocument 404 "The document was not found
```

Verwenden Sie folgende Struktur um eine `ErrorDocument` Einstellung nach Apache HTTP Server 2.0 zu migrieren:

```
ErrorDocument 404 "The document was not found"
```

Beachten Sie, dass in der o.g. Beispiel-Anweisung `ErrorDocument` doppelte Anführungszeichen angehängt wurden.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/core.html#errordocument

10.2.3. Konfiguration des virtuellen Host

Der Inhalt aller `<VirtualHost>` Sektionen sollte auf die gleiche Weise wie der Hauptserver-Abschnitt migriert werden, wie in Abschnitt 10.2.2 beschrieben.

Wichtig

Bitte beachten Sie, dass die SSL/TLS Konfiguration des virtuellen Host aus der Hauptserver-Konfigurationsdatei genommen und in `/etc/httpd/conf.d/ssl.conf` verschoben wurde.

Weitere Informationen zu diesem Thema finden Sie im Kapitel *Apache HTTP Secure Server Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration* und in der Online-Dokumentation unter folgender URL:

- http://httpd.apache.org/docs-2.0/vhosts/

10.2.4. Module und Apache HTTP Server 2.0

In Apache HTTP Server 2.0 wurde das Modulsystem so geändert, dass Module auf neue und interessante Weise miteinander verknüpft und kombiniert werden können. CGI-Skripts sind zum Beispiel in der Lage, serverkonvertierte HTML-Dokumente zu erzeugen, die dann von `mod_include` verarbeitet werden können. Dies eröffnet eine enorme Anzahl von Möglichkeiten in Bezug darauf, wie Module zum Erreichen eines bestimmten Ziels kombiniert werden können.

Das funktioniert so, dass jede Anfrage direkt von einem *handler* Modul bedient wird, gefolgt von null oder mehr *filter* Modulen.

In Apache HTTP Server 1.3, zum Beispiel, würde ein Perl-Skript ganz vom Perl-Modul (`mod_perl`) gehandhabt werden. In Apache HTTP Server 2.0 wird die Anfrage zunächst vom Kernmodul *gehandhabt* — das statische Dateien bedient — und wird dann von `mod_perl` *gefiltert*.

Die genaue Verwendung und alle anderen diesbezüglichen neuen Eigenschaften von Apache HTTP Server 2.0 würden den Rahmen dieses Dokumentes sprengen; die Änderung hat jedoch Auswirkungen, wenn Sie `PATH_INFO` verwendet haben. Darin enthalten sind Pfad-Informationen, die dem echten Dateinamen angehängt werden, in einem Dokument, das von einem jetzt als Filter implementierten Modul gehandhabt wird. Das Kernmodul, das die Anfrage anfangs gehandhabt hat, versteht `PATH_INFO` standardmäßig nicht und wird `404 Not Found` Fehler ausgeben bei Anfragen, die derartige Informationen enthalten. Sie können die Anweisung `AcceptPathInfo` verwenden, um das Kernmodul dazu zu zwingen, Anfragen mit `PATH_INFO` zu akzeptieren.

Untenstehend ein Beispiel dieser Anweisung:

```
AcceptPathInfo on
```

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/core.html#acceptpathinfo
- http://httpd.apache.org/docs-2.0/handler.html
- http://httpd.apache.org/docs-2.0/filter.html

10.2.4.1. Das Modul `mod_ssl`

Die Konfiguration für `mod_ssl` wurde von `httpd.conf` in die Datei `/etc/httpd/conf.d/ssl.conf` verschoben. Damit diese Datei geladen wird und dass folglich `mod_ssl` funktioniert, müssen Sie die Anweisung `Include conf.d/*.conf` wie in Abschnitt 10.2.1.3 beschrieben in Ihrer Datei `httpd.conf` haben.

`ServerName` Anweisungen in virtuellen Hosts von SSL müssen die Port-Nummer ausdrücklich angeben.

Folgendes ist ein Beispiel einer Apache HTTP Server 1.3 Anweisung:

```
<VirtualHost _default_:443>
    # General setup for the virtual host
    ServerName ssl.example.name
    ...
</VirtualHost>
```

Verwenden Sie folgende Struktur um diese Einstellung zu Apache HTTP Server 2.0 zu migrieren:

```
<VirtualHost _default_:443>
    # General setup for the virtual host
    ServerName ssl.host.name:443
    ...
</VirtualHost>
```

Es ist auch wichtig zu beachten, dass beide, die `SSLLog` und `SSLLogLevel` Anweisung, entfernt wurden. Das Modul `mod_ssl` unterliegt nun den `ErrorLog` und `LogLevel` Anweisungen. Sehen Sie Abschnitt 10.5.34 und Abschnitt 10.5.35 für weitere Information zu diesen Anweisungen.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_ssl.html
- http://httpd.apache.org/docs-2.0/vhosts/

10.2.4.2. Das Modul `mod_proxy`

Zugriffskontrollbefehle für den Proxy befinden sich jetzt in einem `<Proxy>` Block anstatt in einem `<Directory proxy:>`.

Die Cache-Funktionalität der alten Datei `mod_proxy` Wurde in folgende drei Module aufgeteilt:

- `mod_cache`
- `mod_disk_cache`
- `mod_mem_cache`

Diese verwenden normalerweise die gleichen oder ähnliche Anweisungen wie die älteren Versionen des `mod_proxy` Moduls, es wird allerdings angeraten jede Anweisung zu prüfen, bevor etwaige Cache-Einstellungen migriert werden.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_proxy.html

10.2.4.3. Das Modul `mod_include`

Das Modul `mod_include` ist jetzt als Filter implementiert (weitere Informationen zu Filtern finden Sie in Abschnitt 10.2.4) und wird deshalb anders aktiviert.

Folgendes ist ein Beispiel einer Apache HTTP Server 1.3 Anweisung:

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Verwenden Sie folgende Struktur um diese Einstellung zu Apache HTTP Server 2.0 zu migrieren:

```
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
```

Beachten Sie bitte, dass die Anweisung `Options +Includes` wie bisher für den <Directory> Abschnitt oder in einer `.htaccess` Datei verlangt wird.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_include.html

10.2.4.4. Die Module `mod_auth_dbm` und `mod_auth_db`

Apache HTTP Server 1.3 unterstützte zwei Authentifizierungsmodule, `mod_auth_db` und `mod_auth_dbm`, die jeweils Berkely-Datenbanken und DBM-Datenbanken verwendeten. Diese Module wurden in Apache HTTP Server 2.0, in ein einziges Modul mit dem Namen `mod_auth_dbm` zusammengefasst, das auf mehrere verschiedene Datenbankformate zugreifen kann. Um von `mod_auth_db` aus Version 1.3 zu migrieren, müssen die Konfigurationsdateien angepasst werden, indem man `AuthDBUserFile` und `AuthDBGroupFile` durch die entsprechenden aus `mod_auth_dbm` ersetzt: `AuthDBMUserFile` und `AuthDBMGroupFile`. Sie müssen außerdem die Anweisung `AuthDBMType DB` hinzufügen um den Typ der Datenbankdatei anzugeben, der verwendet wird.

Folgendes ist ein Beispiel für eine `mod_auth_db` Konfiguration in Apache 1.3:

```
<Location /private/>
  AuthType Basic
  AuthName "My Private Files"
  AuthDBUserFile /var/www/authdb
  require valid-user
</Location>
```

Verwenden Sie folgende Struktur um diese Einstellung zu Apache HTTP Server 2.0 zu migrieren:

```
<Location /private/>
  AuthType Basic
  AuthName "My Private Files"
  AuthDBMUserFile /var/www/authdb
  AuthDBMType DB
  require valid-user
</Location>
```

Bitte beachten Sie, dass die Anweisung `AuthDBMUserFile` auch in `.htaccess` Dateien verwendet werden kann.

Das `dbmmanage` Perl-Skript, das zur Bearbeitung von Benutzernamen- und Passwort-Datenbanken verwendet wurde, wurde in Apache HTTP Server 2.0. durch `htdbm` ersetzt. Das Programm `htdbm`

bietet gleichwertige Funktionalität und kann wie `mod_auth_dbm` mit einer Reihe von Datenbank-Formaten umgehen; die Option `-T` kann in der Befehlszeile zur Bestimmung des Formats verwendet werden.

Tabelle 10-1 zeigt, wie man von einer Datenbank im DBM-Format anhand von `dbmmanage` in das `htdbm` Format migrieren kann.

Aktion	dbmmanage Befehl (Apache 1.3)	Entsprechender htdbm Befehl (Apache 2.0)
Benutzer zu Datenbank hinzufügen (angegebenes Passwort verwenden)	`dbmmanage authdb add username password`	`htdbm -b -TDB authdb username password`
Benutzer zu Datenbank hinzufügen (fragt nach Passwort)	`dbmmanage authdb adduser username`	`htdbm -TDB authdb username`
Benutzer aus Datenbank entfernen	`dbmmanage authdb delete username`	`htdbm -x -TDB authdb username`
Benutzer in Datenbank auflisten	`dbmmanage authdb view`	`htdbm -l -TDB authdb`
Passwort prüfen	`dbmmanage authdb check username`	`htdbm -v -TDB authdb username`

Tabelle 10-1. Migrieren von `dbmmanage` nach `htdbm`

Die Optionen `-m` und `-s` funktionieren sowohl mit `dbmmanage` als auch mit `htdbm` und aktivieren damit jeweils die Verwendung von MD5-oder SHA1-Algorithmen zum Haschieren der Passwörter.

Wird mit `htdbm` eine neue Datenbank erzeugt, muss dies anhand der Option `-c` erfolgen.

Weitere Informationen zu diesem Thema finden Sie in folgender Dokumentation der Apache Software Foundation Website:

- http://httpd.apache.org/docs-2.0/mod/mod_auth_dbm.html

10.2.4.5. Das Modul `mod_perl`

Die Konfiguration für `mod_perl` wurde von `httpd.conf` in die Datei `/etc/httpd/conf.d/perl.conf` verschoben. Damit diese Datei geladen wird und dass folglich `mod_perl` funktioniert, müssen Sie die Anweisung `Include conf.d/*.conf` wie in Abschnitt 10.2.1.3 beschrieben in Ihrer Datei `httpd.conf` haben.

Alle `Apache::` Einträge in `httpd.conf` müssen durch `ModPerl::` ersetzt werden. Außerdem hat sich die Art und Weise geändert, mit der Handler eingetragen werden.

Dies ist ein Beispiel für eine Apache HTTP Server 1.3 `mod_perl` Konfiguration:

```
<Directory /var/www/perl>
    SetHandler perl-script
    PerlHandler Apache::Registry
    Options +ExecCGI
</Directory>
```

Dies entspricht `mod_perl` in Apache HTTP Server 2.0:

```
<Directory /var/www/perl>
```

```
    SetHandler perl-script
    PerlModule ModPerl::Registry
    PerlHandler ModPerl::Registry::handler
    Options +ExecCGI
</Directory>
```

Die meisten Module für `mod_perl` 1.x dürften ohne Änderungen mit `mod_perl` 2.x funktionieren. XS-Module erfordern eine Neukompilierung und bedürfen eventuell geringerer Makefile-Änderungen.

10.2.4.6. Das Modul `mod_python`

Die Konfiguration für `mod_python;` wurde von `/etc/httpd/conf.d/python.conf` verschoben. Damit diese Datei geladen wird und folglich dass `mod_python;` funktioniert, müssen Sie die Anweisung `Include conf.d/*.conf` wie in Abschnitt 10.2.1.3 beschrieben in Ihrer Datei `httpd.conf` haben.

10.2.4.7. PHP

Die Konfiguration für PHP wurde von `httpd.conf` in die Datei `/etc/httpd/conf.d/php.conf` verschoben. Damit diese Datei geladen wird, müssen Sie die Anweisung `Include conf.d/*.conf` wie in Abschnitt 10.2.1.3 beschrieben in Ihrer Datei `httpd.conf` haben.

PHP ist jetzt als Filter implementiert und muss deshalb anders aktiviert werden. Weitere Informationen zu Filtern finden Sie unter Abschnitt 10.2.4.

In Apache HTTP Server 1.3 wurde PHP anhand folgender Anweisungen implementiert:

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
```

Verwenden Sie dagegen in Apache HTTP Server 2.0 folgende Anweisungen:

```
<Files *.php>
    SetOutputFilter PHP
    SetInputFilter PHP
</Files>
```

In PHP 4.2.0 und späteren Versionen haben sich die standardmäßigen vordefinierten Variablen, die im globalen Scope verfügbar waren, geändert. Individuelle Input- und Servervariablen werden nicht mehr standardmäßig direkt in das globale Scope gesetzt. Diese Änderung kann dazu führen, dass Skripts nicht mehr funktionieren. Sie können zum alten Verhalten zurückkehren, indem Sie in der Datei `/etc/php.ini` `register_globals` auf `On` setzen.

Weitere Informationen zu diesem Thema finden Sie im folgenden URL. Darin enthalten sind Einzelheiten zu den Änderungen im globalen Scope:

- http://www.php.net/release_4_1_0.php

10.2.4.8. Das Modul `mod_authz_ldap`

Red Hat Enterprise Linux wird mit dem Modul `mod_authz_ldap` für Apache HTTP Server ausgeliefert. Dieses Modul verwendet die Kurzform des "Distinguished Name" als Subjekt und den Aussteller des Client-SSL-Zertifikats, um den "Distinguished Name" des Benutzers innerhalb eines LDAP-Verzeichnisses zu bestimmen. Es kann auch Benutzer anhand den Attributen der Einträge im LDAP-Verzeichnis autorisieren, wobei Zugriff auf ein Asset auf Benutzerrechte und Gruppenrechten

des Asset basiert und Zugriff für Benutzer mit abgelaufenen Passwörtern abgelehnt wird. Das Modul `mod_ssl` wird für die Verwendung des Modul `mod_authz_ldap` benötigt.

Wichtig

Das Modul `mod_authz_ldap` authetifiziert einen Benutzer zu einem LDAP-Verzecihnis mit einem verschlüsselten Passwort-Hash. Diese Funktionalität ist im experimentellen Modul `mod_auth_ldap` enthalten, das nicht in Red Hat Enterprise Linux enthalten ist. Sehen Sie die Website der Apache Software Foundation Online unter http://www.apache.org/ für Informationen zum Status dieses Moduls.

Die Datei `/etc/httpd/conf.d/authz_ldap.conf` konfiguriert das Modul `mod_authz_ldap`.

Sehen Sie `/usr/share/doc/mod_authz_ldap-`*<version>*`/index.html` (ersetzen Sie *<version>* mit der Versionsnummer des Pakets) für weitere Informationen zur Konfiguration des Moduls `mod_authz_ldap`.

10.3. Nach der Installation

Nach Installieren des `httpd` Pakets, sehen Sie sich die Dokumentation von Apache HTTP Server Online unter http://httpd.apache.org/docs-2.0/ an.

Die Apache HTTP Server-Dokumentation enthält Listen und komplette Beschreibungen aller Konfigurationsoptionen. Um Ihnen die Übersicht zu erleichtern, liefert dieses Kapitel kurze Beschreibungen der von Apache HTTP Server 2.0 verwendeten Konfigurationsanleitungen.

Die Apache HTTP Server-Version 2.0 kann als sicherer Web-Server mit der starken SSL-Verschlüsselung der Pakete `mod_ssl` und `openssl` eingerichtet werden. Beim Lesen der Konfigurationsdateien Ihres Web-Servers stellen Sie sicher, dass diese sowohl den Web-Server ohne, als auch mit Verschlüsselung enthält. Der Web-Server wird als virtueller Host ausgeführt, der in der Datei `/etc/httpd/conf.d/ssl.conf` konfiguriert wird. Weitere Informationen über virtuelle Hosts für sichere Server finden Sie unter Abschnitt 10.8.1. Informationen zur Einrichtung eines sicheren Servers von Apache HTTP finden Sie im Kapitel *Apache HTTP Secure Server Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Bitte beachten

Red Hat, Inc. liefert keine FrontPage-Erweiterungen mit aus, da die Lizenz von Microsoft™ deren Lieferung in einem Produkt eines Drittanbieters verbietet. Mehr über FrontPage-Erweiterungen erfahren Sie unter http://www.rtr.com/fpsupport/.

10.4. Starten und Anhalten von `httpd`

Die `httpd` RPM installiert das `/etc/init.d/httpd`-Skript, auf das Sie anhand des Befehls `/sbin/service` zugreifen können.

Geben Sie folgenden Befehl ein, um Ihren Server als root starten:

```
/sbin/service httpd start
```

Geben Sie folgenden Befehl ein, um Ihren Server anzuhalten:

```
/sbin/service httpd stop
```

Der Befehl `restart` stellt die direkteste Möglichkeit zum Starten und Anhalten dar. Der Befehl `restart` hält den Server an un startet ihn wieder. Beim Neustart werden Sie aufgefordert, Ihr Passwort einzugeben, wenn Sie Apache als Secure Server verwenden.

Der Befehl `restart` stellt sich wie folgt dar:

```
/sbin/service httpd restart
```

Bitte beachten

Wenn Sie Apache HTTP Server als Secure Server ausführen, werden Sie aufgefordert Ihr Passwort bei jeder Verwendung der Optionen `start` oder `restart` einzugeben.

Auch wenn Sie Änderungen in Ihrer Datei `httpd.conf` vorgenommen haben, ist es nicht nötig, dass Sie Ihren Server anhalten und neu starten: zu diesem Zweck können Sie den Befehl `reload` verwenden.

Der Befehl `reload` sieht wie im folgenden Beispiel aus:

```
/sbin/service httpd reload
```

Bitte beachten

Wenn Sie Apache HTTP Server als Secure Server ausführen, brauchen Sie *nicht* Ihr Passwort eingeben, wenn Sie die Option `reload` verwenden, da das Passwort während der neuen Ladevorgänge gespeichert bleibt.

Standardmäßig wird der `httpd` Prozess beim Booten des Rechners *nicht* automatisch gestartet. Sie müssen den `httpd` Service konfigurieren, um beim Booten starten zu können und zwar anhand eines Initskript-Dienstprogrammes wie `/sbin/chkconfig`, **/sbin/ntsysv** oder das **Services Configuration Tool** Programm. Im Kapitel *Controlling Access to Services* im *Red Hat Enterprise Linux Handbuch zur System-Administration* finden Sie weitere Informationen zu diesen Tools.

Bitte beachten

Wenn Sie Apache HTTP Server als Secure Server ausführen, werden Sie nach dem Booten des Rechners nach dem Passwort des Secure Servers gefragt, solange ein verschlüsselter privater SSL-Schlüssel verwendet wird.

Informationen darüber, wie man einen Apache HTTP Secure Server einrichtet, finden Sie im Kapitel *Apache HTTP Secure Server Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

10.5. Konfigurationsanweisungen in `httpd.conf`

Die Apache HTTP Server-Konfigurationsdatei ist `/etc/httpd/conf/httpd.conf`. Die Datei `httpd.conf` enthält ausführliche Kommentare und erklärt sich bis zu einem gewissen Grad selbst. Die Standardkonfiguration Ihres Web-Servers ist für die meisten Situationen ausreichend, Sie sollten sich jedoch mit einigen der wichtigsten Konfigurationsoptionen vertraut machen.

Warnung

Mit der Release von Apache HTTP Server 2.0 haben sich viele Konfigurationsoptionen geändert. Müssen Sie eine Konfigurationsdatei der Version 1.3 in das neue Format migrieren wenden Sie sich an Abschnitt 10.2.

10.5.1. Allgemeine Konfigurationshinweise

Wenn Sie Ihren Apache HTTP Server konfigurieren müssen, ist lediglich die Datei `httpd.conf` zu editieren und anschließend der `httpd.conf`-Prozess neu zu laden oder anzuhalten und neu zu starten. Das Neuladen, Anhalten und Starten von Apache HTTP Server wird in Abschnitt 10.4 besprochen.

Vor dem Editieren von `httpd.conf` sollten Sie zuerst eine Kopie der Originaldatei anlegen. Falls Sie beim Editieren der Konfigurationsdatei einen Fehler machen, steht Ihnen auf diese Weise eine Sicherheitskopie zur Verfügung, mit der Sie von vorn beginnen können.

Falls Sie einen Fehler machen und Ihr Web-Server nicht richtig funktioniert, sollten Sie zuerst die Eingaben der gerade editierten Datei `httpd.conf` überprüfen. Stellen Sie sicher, dass diese keine Tippfehler enthält.

Als Nächstes sollten Sie einen Blick auf die Fehlerprotokolldatei Ihres Web-Servers werfen, `/var/log/httpd/error_log`. Die Auswertung der Fehlerprotokolldatei ist, je nachdem, wie viel Erfahrung Sie damit haben, möglicherweise nicht ganz einfach. Wenn gerade ein Problem aufgetreten ist, sollten die letzten Einträge jedoch einige Hinweise darüber liefern, was passiert ist.

Die folgenden Teilabschnitte enthalten kurze Beschreibungen der Anweisungen in `httpd.conf`. Diese Beschreibungen gehen nicht bis ins letzte Detail. Weitere Informationen finden Sie in der Apache-Dokumentation Online unter http://httpd.apache.org/docs-2.0/.

Weitere Informationen zu `mod_ssl` Anweisungen erhalten Sie aus der Dokumentation Online unter http://httpd.apache.org/docs-2.0/mod/mod_ssl.html.

10.5.2. `ServerRoot`

`ServerRoot` ist das oberste Verzeichnis, das die Server-Dateien enthält. Sowohl der Server mit Verschlüsselung (Secure Server) als auch der Server ohne Verschlüsselung sind auf die Verwendung von `"/etc/httpd"` als `ServerRoot` eingestellt.

10.5.3. `PidFile`

`PidFile` gibt die Datei an, in der der Server seine Prozess-ID (pid) ablegt. Ihr Web-Server ist so konfiguriert, dass er seine pid in `/var/run/httpd.pid` ablegt.

10.5.4. `Timeout`

`Timeout` gibt die Zeit in Sekunden an, die der Server bei Kommunikationsverbindungen auf den Empfang und auf Übertragungen wartet. `Timeout` is auf 300 Sekunden eingestellt, eine für die meisten Situationen geeignete Einstellung.

10.5.5. `KeepAlive`

Mit `KeepAlive` kann eingestellt werden, ob auf Ihrem Server mehr als eine Anfrage pro Verbindung zugelassen ist. `KeepAlive` kann verwendet werden, um zu verhindern, dass ein einzelner Client zu viele der Serverressourcen verbraucht.

Die Standardeinstellung für `KeepAlive` ist `off`. Ist Keepalive auf `on` eingestellt und der Verkehr auf dem Server nimmt spürbar zu, kann der Server schnell die Höchstanzahl von untergeordneten Prozessen erreichen. In dieser Situation lässt die Leistung des Servers deutlich nach. Wenn Keepalive aktiviert ist, ist es ratsam, die Option `KeepAliveTimeout` niedrig einzustellen (siehe Abschnitt 10.5.7) und die Datei `/var/log/httpd/error_log` der Server zu überwachen. Dieses Protokoll erstellt einen Bericht, wenn dem Server keine untergeordneten Prozesse zur Verfügung stehen.

10.5.6. `MaxKeepAliveRequests`

Diese Anweisung gibt an, wie viele Anforderungen pro wiederholter Verbindung maximal erlaubt sind. Die Apache Group empfiehlt einen hohen Wert. Dadurch wird die Leistung des Servers verbessert. Die Standardeinstellung für `MaxKeepAliveRequests` ist `100`, eine für die meisten Situationen geeignete Einstellung.

10.5.7. `KeepAliveTimeout`

`KeepAliveTimeout` gibt in Sekunden an, wie lange der Server wartet, nachdem eine Anforderung bearbeitet wurde. Danach wird die Verbindung getrennt. Nach dem Empfang einer Anforderung gilt stattdessen die Anweisung `Timeout`. Die Vorgabe für `KeepAliveTimeout` ist 15 Sekunden.

10.5.8. `IfModule`

`<IfModule>` und `</IfModule>`-Tags umschließen Anweisungen, die Bedingungen enthalten. Die in den `IfModule`-Tags enthaltenen Anweisungen werden verarbeitet, wenn eine der zwei folgenden Bedingungen erfüllt ist. Die Anweisungen werden verarbeitet, wenn das im ersten `<IfModule>`-Tag enthaltene Modul in den Apache Server geladen wurde. Wenn ein Ausrufezeichen [!] vor dem Modulnamen steht, werden die Anweisungen nur verarbeitet, wenn das Modul im ersten `<IfModule>`-Tag *not* einkompiliert ist.

Weitere Informationen zu Apache HTTP Server-Modulen finden Sie unter Abschnitt 10.7.

10.5.9. MPM spezifische Server-Pool-Anweisungen

Wie in Abschnitt 10.2.1.2, fällt die Verantwortlichkeit für das Management der Server-Pool-Eigenschaften unter Apache HTTP Server 2.0 einer Modul-Gruppe, MPM genannt, zu. Die Eigenschaften des Server-Pool sind unterschiedlich, je nach dem welches MPM verwendet wird. Aus diesem Grund ist ein `IfModule` Container von Nöten, um den Server-Pool für das verwendete MPM zu bestimmen.

Als Vorgabe bestimmt Apache HTTP Server 2.0 den Server-Pool für beide, `prefork` und `worker` MPMs.

Die Folgende ist eine Liste von Anweisungen, die in MPM-spezifischen Server-Pool Containern zu finden sind.

10.5.9.1. `StartServers`

`StartServers` bestimmt, wie viele Serverprozesse beim Start erzeugt werden. Da der Web-Server je nach Datenverkehrsaufkommen Serverprozesse dynamisch beendet bzw. erzeugt, muss dieser Parameter nicht verändert werden. Der Web-Server ist so konfiguriert, dass beim Start `8` Serverprozesse für das `prefork` MPM und `2` für die `worker` MPM erzeugt werden.

10.5.9.2. `MaxRequestsPerChild`

`MaxRequestsPerChild` legt die Gesamtzahl der Anfragen fest, die jeder Child-Server-Prozess benötigt, bevor das Child beendet wird. Der Hauptgrund dür die Einstellung von `MaxRequestsPerChild` ist, dass lang andauernde, durch Prozesse verursachte Speicherlecks vermieden werden sollen. Die Standardeinstellung für `MaxRequestsPerChild` für den Server ist `1000` für das `prefork` MPM und `0` für das `worker` MPM .

10.5.9.3. `MaxClients`

`MaxClients` gibt eine Obergrenze für die Gesamtzahl von Serverprozessen oder gleichzeitig verbundenen Clients an, die zur selben Zeit ausgeführt werden können. Der Hauptgrund für das Bestehen von `MaxClients` ist es zu Verhindern, dass Ihr Betriebssystem durch einen überlasteten Apache HTTP Server-Server zum Absturz gebracht wird. Die Standardeinstellung des Servers ist 150, unabhängig von der verwendeten MPM. Es wird nicht empfohlen `MaxClients` auf einen Wert größer als `256` zu setzen, wenn die `prefork` MPM verwendet wird.

10.5.9.4. `MinSpareServers` and `MaxSpareServers`

Diese Werte werden lediglich mit der `prefork` MPM verwendet und bestimmen wie sich der Apache HTTP Server-Server dynamisch an die erkannte Last anpasst, indem je nach Datenverkehr eine geeignete Anzahl von Reserve-Serverprozessen aufrechterhalten werden. Der Server prüft die Anzahl von Servern, die auf eine Anforderung warten, und beendet einige davon, wenn mehr als von `MaxSpareServers` angegeben vorhanden sind bzw. erzeugt einige neue, wenn weniger als in `MinSpareServers` angegeben vorhanden sind.

Die Standardeinstellung des Servers für `MinSpareServers` ist `5`.Die Standardeinstellung des Servers für `MaxSpareServers` ist `20`. Diese Standardeinstellungen sind für die meisten Situationen geeignet. `MinSpareServers` sollte nicht auf eine zu große Zahl eingestellt werden, weil dadurch selbst bei geringem Datenverkehr die Belastung des Servers hoch ist.

10.5.9.5. `MinSpareThreads` und `MaxSpareThreads`

Diese Werte werden lediglich mit der `worker` MPM verwendet und bestimmen wie sich der Apache HTTP Server-Server dynamisch an die erkannte Last anpasst, indem je nach Datenverkehr eine geeignete Anzahl von Server-Threads in Reserve aufrechterhalten werden. Der Server prüft die Anzahl von Servern, die auf eine Anforderung warten, und beendet einige davon, wenn mehr als von `MaxSpareThreads` angegeben vorhanden sind bzw. erzeugt einige neue, wenn weniger als in `MinSpareThreads` angegeben vorhanden sind.

Die Standardeinstellung des Servers für `MinSpareThreads` ist `25`.Die Standardeinstellung des Servers für `MaxSpareThreads` ist `75`. Diese Standardeinstellungen sind für die meisten Situationen

geeignet. Der Wert für `MaxSpareThreads` muss größer oder gleich der Summe von `MinSpareThreads` und `ThreadsPerChild` sein, oder Apache HTTP Server wird dies automatisch berichtigen.

10.5.9.6. `ThreadsPerChild`

Dieser Wert wird lediglich mit der `worker` MPM verwendet. Er setzt die Anzahl von Threads innerhalb der Child-Prozesse. Der Standardwert für diese Anweisung ist `25`.

10.5.10. `Listen`

Der Befehl `Listen` kennzeichnet den Port, an dem ankommende Anforderungen angenommen werden. Apache HTTP Server ist so konfiguriert, dass auf Port 80 auf unverschlüsselte Web-Kommunikation und (in der Datei `/etc/httpd/conf.d/ssl.conf`, die den Secure Server definiert) auf Port 443 auf sichere Web-Kommunikation gewartet wird.

Wenn Sie Apache HTTP Server so konfigurieren, dass an einem Port kleiner als 1024 gewartet wird, müssen Sie als root angemeldet sein, um den Prozess zu starten. Für Port 1024 und darüber kann `httpd` als normaler Benutzer gestartet werden.

`Listen` kann auch zur Angabe spezieller IP-Adressen verwendet werden, über die der Server Verbindungen annimmt.

10.5.11. `Include`

`Include` erlaubt, dass andere Konfigurationsdateien während der Laufzeit mit aufgenommen werden.

Der Pfad zu diesen Konfigurationspfaden kann absolut sein oder sich auf `ServerRoot` beziehen.

Wichtig

Damit der Server einzeln verpackte Module verwendet, wie `mod_ssl`, `mod_perl` und `php`, muss sich folgende Anweisung in `Section 1: Global Environment` von `http.conf` befinden:

```
Include conf.d/*.conf
```

10.5.12. `LoadModule`

`LoadModule` wird verwendet um Dynamic Shared Objects (DSO)-Modulen zu laden. Weitere Informationen zur DSO-Unterstützung von Apache HTTP Server einschließlich der genauen Verwendung der Anweisung `LoadModule` finden Sie in Abschnitt 10.7. Beachten Sie, dass die Ladereihenfolge der Module *nicht länger* wichtig ist bei Apache HTTP Server 2.0. Weitere Informationen zur DSO-Unterstützung in Apache HTTP Server 2.0 finden Sie unter Abschnitt 10.2.1.3.

10.5.13. `ExtendedStatus`

Die Anweisung `ExtendedStatus` bestimmt, ob Apache beim Aufruf des `server-status`-Handler grundlegende (`off`) oder detaillierte Server-Status-Informationen (`on`) erstellt. `Server-status` wird über `Location`-Tags aufgerufen. Weitere Informationen zum Aufruf von `server-status` finden Sie in Abschnitt 10.5.59.

10.5.14. `IfDefine`

Die Tags <IfDefine> und </IfDefine> umschließen Konfigurationsanweisungen, die ausgeführt werden, wenn sich für die Bedingung im Tag <IfDefine> die Aussage wahr ergibt. Die Anweisungen werden nicht ausgeführt, wenn sich die Aussage falsch ergibt.

Die Bedingung in den Tags <IfDefine> ist eine Parameterbezeichnung (z.B. HAVE_PERL). Wenn der Parameter definiert ist, d.h. er wurde beim Start des Servers als Argument des Startbefehls angegeben, ist die Aussage wahr. In diesem Fall ist die Bedingung wahr, wenn Ihr Web-Server gestartet ist, und die Anweisungen in den Tags IfDefine werden ausgeführt.

10.5.15. `User`

Die Anweisung User definiert die Benutzer-ID, die vom Server zur Beantwortung von Anforderungen verwendet wird. Die User-Einstellung bestimmt die Zugriffsrechte des Servers. Alle Dateien, auf die dieser Benutzer nicht zugreifen darf, sind für die Besucher Ihrer Website ebenfalls nicht zugänglich. Die Standardeinstellung für User ist apache.

Der User sollte nur Zugriffsrechte auf solche Dateien haben, die für die Außenwelt sichtbar sein sollen. Der in User eingetragene Benutzer ist auch der Eigentümer aller vom Server erzeugten CGI-Prozesse. Der in User eingetragene Benutzer sollte nur Codes ausführen dürfen, die zur Beantwortung von HTTP-Anforderungen vorgesehen sind.

Bitte beachten

Aus Sicherheitsgründen kann Apache HTTP Server nicht als root-Benutzer ausgeführt werden.

10.5.16. `Group`

Die Anweisung Group legt den Gruppennamen der Apache HTTP Server-Prozesse fest.

Die Standardeinstellung für Group ist apache.

10.5.17. `ServerAdmin`

ServerAdmin sollte auf die E-Mail-Adresse Ihres Web-Server-Administrators eingestellt sein. Diese E-Mail-Adresse wird in Fehlermeldungen auf vom Server erstellten Web-Seiten angezeigt, damit die Benutzer dem Serveradministrator ein Problem per E-Mail melden können.

ServerAdmin ist standardmäßig root@localhost.

Meistens ist es am günstigsten, ServerAdmin auf webmaster@example.com einzustellen. Richten Sie dann in /etc/aliases einen Alias webmaster ein, der auf den für den Web-Server Verantwortlichen zeigt. Führen Sie schließlich /usr/bin/newaliases aus, um den neuen Alias hinzuzufügen.

10.5.18. `ServerName`

Mit ServerName können Sie einen Rechnernamen und eine Port-Nummer (die mit der Anweisung Listen übereinstimmt) für Ihren Server angeben. Der Servername kann sich vom vom wirklichen Namen Ihres Host unterscheiden. Zum Beispiel können Sie so den Namen www.your_domain.com

einrichten, obwohl der wirkliche Name Ihres Servers foo.your_domain.com. Beachten Sie, dass `ServerName` einen gültigen Domain Name Service (DNS)-Namen enthalten muss, den Sie auch tatsächlich verwenden dürfen — also nicht einfach etwas ausdenken.

Zum Beispiel:

```
ServerName www.example.com:80
```

Wenn Sie in `ServerName` einen Servernamen angeben, muss die entsprechende Zuordnung von IP-Adresse und Servername in Ihrer `/etc/hosts`-Datei enthalten sein.

10.5.19. `UseCanonicalName`

Wenn auf `on` gesetzt, konfiguriert diese Anweisung Apache HTTP Server dazu, sich selbst mit den `ServerName` und `Port` Anweisungen zu referenzieren. Ist `UseCanonicalName` auf `off` gesetzt, verwendet der Server stattdessen den Wert, der in der Anforderung des Clients enthalten ist, um sich selbst zu referenzieren.

`UseCanonicalName` ist standardmäßig auf `off` eingestellt.

10.5.20. `DocumentRoot`

`DocumentRoot` ist das Verzeichnis, das die meisten HTML-Dateien enthält, die der Server auf Anforderung überträgt. Der Standardeintrag für `DocumentRoot` ist sowohl für den unverschlüsselten als auch für den Secure Web-Server `/var/www/html`. Zum Beispiel könnte der Server eine Anforderung für folgendes Dokument empfangen:

```
http://example.com/foo.html
```

Der Server sucht die folgende Datei im Standardverzeichnis:

```
/var/www/html/foo.html
```

Wenn Sie den Eintrag in `DocumentRoot` ändern möchten, dass dieser nicht vom sicheren und vom unverschlüsselten Web-Server gemeinsam benutzt wird, finden Sie in Abschnitt 10.8 entsprechende Informationen.

10.5.21. `Directory`

Die Tags `<Directory /path/to/directory>` und `</Directory>` werden verwendet, um eine Gruppe von Konfigurationsanweisungen zu umschließen, die sich nur auf dieses Verzeichnis und alle seine Unterverzeichnisse beziehen sollen. Alle Anweisungen, die auf ein Verzeichnis anwendbar sind, können innerhalb der `<Directory>`-Tags verwendet werden.

In der Standardeinstellung werden für das root-Verzeichnis mit den Anweisungen `Options` (siehe Abschnitt 10.5.22) und `AllowOverride` (siehe Abschnitt 10.5.23) sehr restriktive Parameter vorgegeben. Bei dieser Konfiguration müssen für jedes Verzeichnis die Einstellungen explizit vergeben werden, wenn weniger restriktive Einstellungen erforderlich sind.

Mit `Directory`-Tags werden für `DocumentRoot` weniger restriktive Parameter definiert, damit HTTP-Anforderungen in diesem Verzeichnis bearbeitet werden können.

Das Verzeichnis `cgi-bin` wird mit der Option `ExecCGI`für die Ausführung von CGI-Skripts eingerichtet.

Wenn die Ausführung von CGI-Skripts in anderen Verzeichnissen erforderlich ist, müssen Sie `ExecCGI` entsprechend für dieses Verzeichnis einstellen.

Wenn Ihr Verzeichnis `cgi-bin` zum Beispiel `/var/www/cgi-bin` ist, Sie aber CGI-Skripts im Verzeichnis `/home/my_cgi_directory` ausführen möchten, können Sie in Ihrer Datei `httpd.conf` eine `ExecCGI`-Anweisung mit einem Satz von `Directory`-Anweisungen hinzufügen:

```
<Directory /home/my_cgi_directory>
    Options +ExecCGI
</Directory>
```

Als nächstes muss das Kommentar aus der `AddHandler` Anweisung entfernt werden, um Dateien mit der Endung `.cgi` als CGI-Skripte zu identifizieren. Sehen Sie Abschnitt 10.5.55 für Anleitungen zum Setzen von `AddHandler`.

Die Zugriffsberechtigungen für CGI-Skripts und den gesamten Pfad zu den Skripts müssen auf 0755 eingestellt sein.

10.5.22. `Options`

Die Anweisung `Options` bestimmt, welche Serverfunktionen in einem bestimmten Verzeichnis verfügbar sind. Zum Beispiel ist für `Options` entsprechend den restriktiven Parametern für das root-Verzeichnis lediglich `FollowSymLinks` angegeben. Es sind keine Funktionen aktiviert, außer dass der Server im root-Verzeichnis symbolischen Links folgen darf.

In Ihrem Verzeichnis `DocumentRoot` ist `Options` standardmäßig so konfiguriert, dass `Indexes`, `Includes` und `FollowSymLinks` enthalten sind. `Indexes` erlaubt dem Server, eine Verzeichnisliste für ein Verzeichnis zu erstellen, wenn kein `DirectoryIndex` (z.B. `index.html`) angegeben wird. `Includes` bedeutet, dass server-seitige Includes erlaubt sind. `FollowSymLinks` erlaubt dem Server, in diesem Verzeichnis symbolischen Links zu folgen.

Bitte beachten

`Options` statements from the main server configuration section needs to be replicated to each `VirtualHost` containers individually. Refer to Abschnitt 10.5.65 for more information about `VirtualHost` containers.

10.5.23. `AllowOverride`

Die Anweisung `AllowOverride` bestimmt, ob `Options` durch Deklarationen in einer `.htaccess`-Datei überschrieben werden können. Standardmäßig sind sowohl das root-Verzeichnis als auch `DocumentRoot`so konfiguriert, dass ein Überschreiben durch `.htaccess` nicht möglich ist.

10.5.24. `Order`

Die Anweisung `Order` bestimmt die Reihenfolge, in der die Anweisungen `allow` und `deny` ausgewertet werden. Der Server ist so konfiguriert, dass für Ihr `Allow`>-Anweisungen vor den `Deny` -Anweisungen für Ihr `DocumentRoot` ausgewertet werden.

10.5.25. Allow

Allow gibt an, welcher Anforderer auf ein bestimmtes Verzeichnis zugreifen darf. Der Anforderer kann sein: all, ein Domänenname, eine IP-Adresse, ein Teil einer IP-Adresse, ein Netzwerk-/Netmask-Paar usw. Ihr DocumentRoot-Verzeichnis ist so konfiguriert, dass durch Allow Anforderungen von all (d.h. allen Anforderern) erlaubt sind.

10.5.26. Deny

Deny funktioniert genauso wie Allow, wobei angegeben wird, wem der Zugriff nicht gestattet ist. In Ihrer DocumentRoot sind standardmäßig keine Deny-Anweisungen enthalten.

10.5.27. UserDir

UserDir ist der Name des Unterverzeichnisses innerhalb eines Home-Verzeichnisses jedes Benutzers, wo private HTML-Seiten abgelegt werden können, die vom Web-Server bereitgestellt werden sollen. Diese Anweisung hat den Standardwert disable.

Die Standardeinstellung für das Unterverzeichnis ist public_html. Zum Beispiel könnte der Server die folgende Anforderung erhalten:

```
http://example.com/~username/foo.html
```

Der Server sucht daraufhin die Datei:

```
/home/username/public_html/foo.html
```

Im obigen Beispiel ist /home/username das Home-Verzeichnis des Benutzers. (Beachten Sie bitte, dass der Standardpfad zu den Home-Verzeichnissen von Benutzern auf Ihrem System abweichen kann.)

Überprüfen Sie, ob die Zugriffsberechtigungen für die Home-Verzeichnisse der Benutzer richtig eingestellt sind. Die richtige Einstellung ist 0711. Für die public_html-Verzeichnisse der Benutzer müssen die read (r)- und execute (x)-Bits eingestellt sein (0755 ist ebenfalls ausreichend). Dateien, die im public_html-Verzeichnis der Benutzer zum Abruf angeboten werden, müssen mindestens die Berechtigung 0644 haben.

10.5.28. DirectoryIndex

Der DirectoryIndex ist die Standardseite, die vom Server geliefert wird, wenn ein Benutzer durch Angabe von "/" am Ende eines Verzeichnisnamens einen Index eines Verzeichnisses anfordert.

Wenn ein Benutzer zum Beispiel die Seite http://*example*/*this_directory*/, anfordert, wird entweder die DirectoryIndex-Seite (falls vorhanden) oder eine vom Server erstellte Verzeichnisliste angezeigt. Die Standardeinstellung für den DirectoryIndex ist index.html und die index.html.var Type-Map. Der Server sucht nach diesen Dateien und gibt die Datei aus, die zuerst gefunden wird. Wenn keine dieser Dateien gefunden wird und Options Indexes für dieses Verzeichnis aktiviert ist, erstellt und überträgt der Server eine Liste im HTML-Format, die die Unterverzeichnisse und Dateien im Verzeichnis enthält.

10.5.29. AccessFileName

AccessFileName bestimmt die Datei, die vom Server zur Speicherung von Zugriffskontrollinformationen in jedem Verzeichnis verwendet werden soll. Standardmäßig ist Ihr Web-Server so konfiguriert,

dass für die Speicherung von Zugriffskontrollinformationen die Datei `.htaccess` verwendet wird (falls vorhanden).

Unmittelbar nach der Anweisung `AccessFileName` wird durch eine Reihe von `Files`-Tags die Zugangskontrolle zu allen Dateien geregelt, die mit `.ht` beginnen. Diese Anweisungen verwehren aus Sicherheitsgründen den Zugriff auf alle `.htaccess`-Dateien (bzw. andere Dateien, die mit which begin with `.ht` beginnen.

10.5.30. `CacheNegotiatedDocs`

Standardmäßig fordert Ihr Web-Server Proxyserver auf, keine Dokumente im Cache zu halten, die auf der Grundlage des Inhalts übertragen wurden (d.h. sie können nach einer gewissen Zeit oder aufgrund der Eingabe des Anforderers geändert werden). Wenn Sie `CacheNegotiatedDocs` auf `on` setzen, wird diese Funktion deaktiviert und Proxyserver können Dokumente im Cache halten.

10.5.31. `TypesConfig`

`TypesConfig` gibt die Datei an, die die Standardliste der MIME Type-Zuordnungen definiert (Dateinamenerweiterungen für Inhaltstypen). Die Standarddatei für `TypesConfig` ist `/etc/mime.types`. Es wird empfohlen, zum Hinzufügen von MIME Type-Zuordnungen die Datei `/etc/mime.types`nicht zu editieren, sondern die Anweisung `AddType` zu verwenden.

Weitere Informationen über `AddType` finden Sie in Abschnitt 10.5.54.

10.5.32. `DefaultType`

`DefaultType` definiert einen Standardinhaltstyp, den der Web-Server für Dokumente verwendet, deren MIME-Types nicht bestimmt werden können. Die Standardeinstellung für Ihren Web-Server ist, dass bei Dateien mit einem nicht genau zu bestimmenden Inhaltstyp ein Standardtext-Inhaltstyp angenommen wird.

10.5.33. `HostnameLookups`

`HostnameLookups` kann auf `on`, `off` oder `double` eingestellt werden. Wenn Sie `HostnameLookups` erlauben (durch Einstellung auf `on`), wird vom Server die IP-Adresse für jede Verbindung, die ein Dokument von Ihrem Web-Server anfordert, automatisch aufgelöst. Die Auflösung der IP-Adresse bedeutet, dass Ihr Server mindestens eine Verbindung zum DNS herstellt, um den zu einer IP-Adresse gehörenden Host-Namen zu bestimmen. Wenn Sie `HostnameLookups` auf `double` einstellen, stellt Ihr Server einen doppelt-umgekehrten DNS aus. Mit anderen Worten: nach einem umgekehrten Lookup wird ein Vorwärts-Lookup ausgeführt. Mindestens eine der IP-Adressen im Vorwärts-Lookup muss der Adresse des ersten umgekehrten Lookup entsprechen.

Im Allgemeinen sollten Sie die Einstellung für `HostnameLookups` auf `off` belassen, um Ressourcen zu sparen.

Wenn Sie sich die Host-Namen in Ihrer Protokolldai ansehen wollen, verwenden Sie eines der vielen Protokolldateinanalysier-Tools, mit denen die DNS-Lookups wirkungsvoller und stapelweise erfolgt wenn Sie Ihre Protokolldatein rotieren.

10.5.34. `ErrorLog`

`ErrorLog` bestimmt die Datei, in der Server-Fehler protokolliert werden. Wie durch den Namen der Anweisung angedeutet, ist die Fehlerprotokolldatei für Ihren Web-Server `/var/log/httpd/error_log`.

10.5.35. LogLevel

`LogLevel` legt fest, wie ausführlich die Fehlermeldungen im Fehlerprotokoll dargestellt werden. `LogLevel` kann auf `emerg`, `alert`, `crit`, `error`, `warn`, `notice`, `info` oder `debug` eingestellt werden (von der kürzesten bis zur ausführlichsten Darstellung). `LogLevel` ist standardmäßig auf `warn` eingestellt.

10.5.36. LogFormat

Die `LogFormat`-Anweisung bestimmt das Format in den verschiedenen Web-Server Log-Dateien. Welches `LogFormat` verwendet wird, hängt von den Einstellungen in der `CustomLog`-Anweisung ab (siehe Abschnitt 10.5.37).

The following are the format options if the `CustomLog` directive is set to `combined`:

`%h` (remote host's IP address or hostname)

Lists the remote IP address of the requesting client. If `HostnameLookups` is set to `on`, the client hostname is recorded unless it is not available from DNS.

`%l` (rfc931)

Not used. A hyphen [-] appears in the log file for this field.

`%u` (authenticated user)

If authentication was required, lists the user name of the user is recorded. Usually, this is not used, so a hyphen [-] appears in the log file for this field.

`%t` (date)

Lists the date and time of the request.

`%r` (request string)

Lists the request string exactly as it came from the browser or client.

`%s` (status)

Lists the HTTP status code which was returned to the client host.

`%b` (bytes)

Lists the size of the document.

`%\"%{Referer}i\"` (referrer)

Lists the URL of the webpage which referred the client host to Web server.

`%\"%{User-Agent}i\"` (user-agent)

Lists the type of Web browser making the request.

10.5.37. CustomLog

`CustomLog` bestimmt die Protokolldatei und das Protokolldateiformat. In der Standardkonfiguration Ihres Web-Servers bestimmt `CustomLog` die Protokolldatei, in der die Zugriffe auf Ihren Web-Server protokolliert werden: `/var/log/httpd/access_log`. Wenn Sie für Ihren Web-Server Server-Leistungsstatistiken auf der Basis der Zugriffe erstellen möchten, muss Ihnen bekannt sein, wo diese Datei abgelegt ist.

`CustomLog` stellt außerdem das Protokolldateiformat auf "common" ein. Das Protokolldateiformat "common" sieht folgendermaßen aus:

```
remotehost rfc931 user date "request" status bytes referrer user-agent
```

10.5.38. `ServerSignature`

Die Anweisung `ServerSignature` fügt in alle vom Server erstellten Dokumente eine Zeile ein, die die Apache Serverversion und den `ServerName` des Rechners enthält, auf dem der Server ausgeführt wird (z.B. Fehlermeldungen, die an Clients zurückgesendet werden). `ServerSignature` ist standardmäßig auf `on` eingestellt.

Sie können die Einstellung auf `off` setzen, oder auf `EMail`, was einen `mailto:ServerAdmin` HTML-Tag in die Signaturzeile einfügt.

10.5.39. `Alias`

Mit der Einstellung `Alias` können Verzeichnisse außerhalb des Verzeichnisses `DocumentRoot` liegen und der Web-Server kann dennoch darauf zugreifen. Jede URL, die mit dem Alias endet, verzweigt automatisch zum Aliaspfad. Als Standard- Einstellung ist bereits ein Alias eingerichtet. Auf das Verzeichnis `icons/` kann vom Web-Server zugegriffen werden, liegt liegt jedoch nicht `DocumentRoot`.

10.5.40. `ScriptAlias`

Die Einstellung `ScriptAlias` legt fest, wo CGI-Skripts (oder andere Skriptarten) abgelegt sind. Im Allgemeinen sollten CGI-Skripts nicht in `DocumentRoot` abgelegt werden. In `DocumentRoot` abgelegte CGI-Skripts könnten wie Textdokumente gelesen werden. Auch wenn Sie nichts dagegen haben, dass andere Ihre CGI-Skripts lesen und weiterverwenden, könnte die Offenlegung ihrer Funktion von Benutzern mit krimineller Energie zur Ausnutzung von Sicherheitslücken im Skript genutzt werden. Dies kann somit ein Sicherheitsrisiko für Ihren Server darstellen. Standardmäßig ist das Verzeichnis `cgi-bin` ein `ScriptAlias` von `/cgi-bin/` und in Wirklichkeit das Verzeichnis `/var/www/cgi-bin/`.

Hinweise zum Ausführen von CGI-Skripts in anderen Verzeichnissen als `cgi-bin` finden Sie in Abschnitt 10.5.55 und Abschnitt 10.5.21.

10.5.41. `Redirect`

Wenn eine Web-Seite verschoben wird, kann mit `Redirect` die Zuordnung der alten URL auf eine neue URL erfolgen. Hier das Format:

```
Redirect /<old-path>/<file-name> http://<current-domain>/<current-path>/<file-name>
```

Wenn also eine HTTP-Anforderung für eine Seite empfangen wird, die früher unter http://*your_domain*/*path*/foo.html abgerufen werden konnte, sendet der Server die neue URL (http://*new_domain*/*path*/foo.html) an den Client, der dann im Normalfall versucht, das Dokument von der neuen URL abzurufen.

In this example, any requests for <*file-name*> at the old location is automatically redirected to the new location.

Genauere Hinweise zur Redirect-Option finden Sie im Modul `mod_rewrite`, das mit dem Server geliefert wird.

10.5.42. IndexOptions

IndexOptions bestimmt das Erscheinungsbild der vom Server erstellten Verzeichnislisten durch das Hinzufügen von Symbolen, Dateibeschreibungen usw. Wenn Options Indexes aktiviert ist (siehe Abschnitt 10.5.22), kann Ihr Web-Server eine Verzeichnisliste erstellen, wenn er eine HTTP-Anforderung wie die Folgende empfängt:

http://*your_domain*/*this_directory*/

Die Standardkonfiguration schaltet FancyIndexing ein. Das heisst, dass ein Benutzer ein Verzeichnis durch Klicken auf die Spaltenheader neu ordnen kann. Ein weiterer Klick auf den selben Header ändert die Reihenfolge von Aufsteigend nach Absteigend. FancyIndexing zeigt auch verschiedene Icons für verschiedene Dateien, je nach Dateiendungen.

In der Standardkonfiguration ist FancyIndexing aktiviert. Wenn FancyIndexing aktiviert ist, werden durch Klicken auf die Überschrift der Spalte in der Verzeichnisliste die Einträge entsprechend dieser Spalte sortiert. Ein weiterer Klick auf dieselbe Überschrift schaltet von aufsteigender zu absteigender Reihenfolge um und umgekehrt. FancyIndexing zeigt außerdem je nach Dateiendung verschiedene Symbole für verschiedene Dateien an. Bei Verwendung der Anweisung AddDescription und aktiviertem FancyIndexing wird in der vom Server erstellten Verzeichnisliste eine kurze Dateibeschreibung angegeben.

IndexOptions hat eine Reihe von weiteren Parametern, die zur Festlegung des Erscheinungsbilds der vom Server erstellten Verzeichnisse verwendet werden können. Zu diesen Parametern gehören IconHeight und IconWidth, durch die der Server angewiesen wird, die HTML-Tags HEIGHT und WIDTH für die Symbole in vom Server erstellten Web-Seiten zu verwenden, sowie IconsAreLinks,durch die die Symbole zusammen mit dem Dateinamen als Teil des HTML-Ankers für den Link verwendet werden können.

10.5.43. AddIconByEncoding

Diese Anweisung bestimmt die Symbole, die in vom Server erstellten Verzeichnislisten für Dateien mit MIME-Encoding angezeigt werden. Zum Beispiel verwendet der Web-Server in vom Server erstellten Verzeichnislisten standardmäßig für MIME-codierte x-compress- und x-gzip-Dateien das Symbol compressed.gif.

10.5.44. AddIconByType

In dieser Anweisung werden Symbole angegeben, die in vom Server erstellten Verzeichnislisten für Dateien mit MIME-Types angezeigt werden. Ihr Server ist zum Beispiel so konfiguriert, dass in vom Server erstellten Verzeichnislisten für Dateien mit dem Mime-Type "text"; das Symbol text.gif angezeigt wird.

10.5.45. AddIcon

AddIcon gibt an, welche Symbole in vom Server erstellten Verzeichnislisten für bestimmte Dateitypen bzw. für Dateien mit bestimmten Erweiterungen anzuzeigen sind. Zum Beispiel ist Ihr Web-Server so konfiguriert, dass das Symbol binary.gif für Dateien mit der Erweiterung .bin oder .exe verwendet wird.

10.5.46. DefaultIcon

DefaultIcon bestimmt das Symbol, das in vom Server erstellten Verzeichnislisten für Dateien angezeigt wird, für die kein anderes Symbol angegeben ist. unknown.gif ist für diese Dateien standardmäßig DefaultIcon.

10.5.47. AddDescription

Mit AddDescription können Sie in vom Server erstellten Listen für bestimmte Dateien von Ihnen eingegebenen Text anzeigen lassen (dazu muss außerdem FancyIndexing in IndexOptions) aktiviert sein). Sie können bestimmte Dateien, Wildcards oder Dateiendungen für die Dateien angeben, auf die diese Anweisung angewandt werden soll.

10.5.48. ReadmeName

ReadmeName bestimmt die Datei, die an das Ende der vom Server erstellten Verzeichnisliste angehängt wird (falls die Datei im Verzeichnis vorhanden ist). Der Web-Server versucht zuerst, die Datei als HTML-Dokument anzuhängen, dann als Standardtextdatei. Standardmäßig ist ReadmeName auf README eingestellt.

10.5.49. HeaderName

HeaderName bestimmt die Datei, die am Beginn der vom Server erstellten Verzeichnislisten eingefügt wird (falls die Datei im Verzeichnis vorhanden ist). Wie bei ReadmeName versucht der Server, die Datei nach Möglichkeit als HTML-Datei anzuhängen, sonst als einfachen Text.

10.5.50. IndexIgnore

IndexIgnore kann Dateiendungen, Teile von Dateinamen, Wildcards oder vollständige Dateinamen enthalten. Der Web-Server nimmt Dateien, die diesen Parametern entsprechen, nicht mit in vom Server erstellte Verzeichnislisten auf.

10.5.51. AddEncoding

AddEncoding bestimmt, welche Dateinamenerweiterungen eine spezielle Codierungsart angeben sollen. AddEncoding kann auch bei manchen Browsern (nicht bei allen) dazu verwendet werden, bestimmte Dateien beim Download zu entpacken.

10.5.52. AddLanguage

AddLanguage verknüpft Dateinamenserweiterungen mit der speziellen Sprache, in der der Inhalt abgefasst ist. Diese Anweisung ist hauptsächlich für den Inhaltsabgleich nützlich, wenn der Server je nach Spracheinstellung im Browser des Clients eines von mehreren möglichen Dokumenten zurückliefert.

10.5.53. LanguagePriority

LanguagePriority ermöglicht die Einstellung, in welchen Sprachen Dateien geliefert werden sollen, falls vom Client im Browser keine Angabe zur Sprache vorliegt.

10.5.54. AddType

Verwenden Sie die AddType-Anweisung, um die Paare von MIME-Type und Dateiendung zu bestimmen, oder die Standardeinstellungen zu überschreiben. Die folgenden Beispielsanweisungen weisen Apache HTTP Server an die Dateiendung .tgz zu kennen:

```
AddType application/x-tar .tgz
```

10.5.55. AddHandler

`AddHandler` ordnet Dateierweiterungen speziellen Handlern zu. Der `cgi-script`-Handler kann zum Beispiel in Kombination mit der Erweiterung `.cgi` verwendet werden, um eine Datei mit der Endung `.cgi` als CGI-Skript zu bearbeiten. Das funktioniert auch für Dateien, die außerhalb des Verzeichnisses `ScriptAlias` liegen, wenn Sie die hier angegebenen Hinweise beachten. Ihre Datei `httpd.conf` enthält einen `AddHandler` für CGI:

```
AddHandler cgi-script .cgi
```

Zusätzlich muss `ExecCGI` als `Options` für alle Verzeichnisse eingestellt werden, die ein CGI-Skript enthalten. Weitere Informationen zum Einstellen von `ExecCGI` für ein Verzeichnis finden Sie in Abschnitt 10.5.21.

`AddHandler` wird vom Server neben CGI-Skripts auch für die Verarbeitung der vom Server verarbeiteten HTML- und Imagemap-Dateien verwendet.

10.5.56. Action

`Action` ermöglicht die Angabe einer Paarung aus MIME-Inhaltstyp und CGI-Skript, damit ein spezielles CGI-Skript immer dann ausgeführt wird, wenn eine Datei dieses Medientyps angefordert wird.

10.5.57. ErrorDocument

`ErrorDocument` verknüpft einfach einen HTTP-Antwortcode mit einer Meldung oder einer URL, die zum Client zurückgesendet wird. Standardmäßig gibt Ihr Web-Server bei einem Problem oder Fehler eine einfache und meist kryptische Fehlermeldung an den anfordernden Client zurück. Statt der Standardeinstellung können Sie `ErrorDocument` zur Konfiguration Ihres Web-Servers verwenden, so dass der Server eine von Ihnen angepasste Meldung ausgibt oder den Client zu einer lokalen oder externen URL umleitet.

Wichtig

Sie *müssen* die Fehlermeldung in doppelte Anführungszeichen ["] setzen, damit sie gütig ist.

10.5.58. BrowserMatch

Die Anweisung `BrowserMatch` ermöglicht es Ihrem Server, Umgebungsvariablen zu definieren und auf Grundlage des User-Agent HTTP-Header-Felds (gibt den Browser des Clients an) in geeigneter Weise zu reagieren. Standardmäßig verwendet Ihr Web-Server `BrowserMatch`, um keine Verbindungen mit Browsern zuzulassen, die Probleme bereiten, und zum Deaktivieren von Keepalives und HTTP-Header-Löschbefehlen für Browser, von denen bekannt ist, dass sie Probleme mit diesen Aktionen haben.

10.5.59. `Location`

Die Tags `<Location>` und `</Location>` ermöglichen die Angabe von Zugangsberechtigungen auf URL-Basis.

Wenn Sie zulassen möchten, dass Benutzer von Ihrer Domäne aus Serverstatusberichte einsehen können, sollten Sie für den nächsten Abschnitt mit Anweisungen die Kommentare entfernen:

```
<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from <.example.com>
</Location>
```

Dabei muss `.your_domain.com` durch den Namen Ihrer Second Level-Domäne ersetzt werden.

Wenn Sie Serverkonfigurationsberichte (einschließlich installierter Module und Konfigurationsanweisungen) für Anforderungen aus Ihrer Domäne bereitstellen möchten, müssen für die folgenden Zeilen die Kommentare entfernt werden:

```
<Location /server-info>
    SetHandler server-info
    Order deny,allow
    Deny from all
    Allow from <.example.com>
</Location>
```

Auch hier muss `.your_domain.com` entsprechend angegeben werden.

10.5.60. `ProxyRequests`

Um den Apache HTTP Server als Proxy-Server zu konfigurieren, entfernen Sie das Hash-Symbol (`#`) vom Anfang der Zeile `<IfModule mod_proxy.c>`, den ProxyRequests und jeder Zeile in der `<Proxy>`-Stanza. Setzen Sie die `ProxyRequests`-Anweisung auf `On` und geben Sie an, welchen Domains Zugriff zum Server in der `Allow from`-Anweisung der `<Proxy>`-Stanza erlaubt sind.

10.5.61. `Proxy`

`<Proxy *>` and `</Proxy>` tags create a container which encloses a group of configuration directives meant to apply only to the proxy server. Many directives which are allowed within a `<Directory>` container may also be used within `<Proxy>` container.

10.5.62. `ProxyVia`

Der Befehl `ProxyVia` legt für eine HTTP Via:-Zeile fest, ob diese zusammen mit Anforderungen oder Antworten gesendet wird, die über den Apache Proxyserver laufen. Der Header Via: enthält den Host-Namen, wenn `ProxyVia` auf `On` eingestellt ist, den Host-Namen und die Apache HTTP Server Version bei Einstellung auf `Full`, alle Via:-Zeilen werden unverändert weitergegeben bei Einstellung auf `Off` und die Via:-Zeilen werden entfernt bei Einstellung auf `Block`.

10.5.63. Cache-Anweisungen

Eine Reihe von Cache-Anweisungen sind in in der Standard-Konfigurationsdatei von Apache HTTP Server enthalten. In den meisten Fällen reicht es aus, das Hash-Symbol (`#`) vom Anfang der Zeile zu entfernen. Die folgenden sind jedoch einige wichtigere Cache-Anweisungen.

- `CacheEnable` — Gibt an, ob der Cache ein Platten-, Speicher- oder Datei-Cache ist. Als Vorgabe konfiguriert `CacheEnable` einen Platten-Cache für URLs auf oder unterhalb `/`.
- `CacheRoot` bestimmt den Namen des Verzeichnisses, in dem die zwischengespeicherten Dateien abgelegt werden. Die Standard-`CacheRoot` ist `/var/cache/httpd`.
- `CacheSize` bestimmt, wie viel Speicherplatz in KB für den Cache zur Verfügung gestellt wird. Der Standardwert für `CacheSize` ist `5` KB.

Die folgende Liste gibt einige andere Cache-bezogene Anweisungen.

- `CacheMaxExpire` — Im Cache gespeicherte HTML-Dokumente werden für eine maximale Anzahl von Stunden, durch diese Anweisung angegeben, im Cache gehalten (ohne Neuladen vom Ursprungsserver). Der Standardwert ist `24` Stunden (`86400` seconds).
- Der `CacheLastModifiedFactor` betrifft die Erzeugung eines Ablaufdatums (expiration) für ein Dokument, das vom Ursprungsserver nicht mit einem eigenen Ablaufdatum versehen wurde. Der Standard-`CacheLastModifiedFactor` ist auf `0.1` eingestellt, d.h. das Ablaufdatum für solche Dokumente entspricht einem Zehntel der Zeit, die vergangen ist, seitdem das Dokument zuletzt geändert wurde.
- `CacheDefaultExpire` — Die Ablaufzeit in Stunden für ein Dokument, das über ein Protokoll empfangen wurde, das keine Ablaufzeiten unterstützt. Die Standardeinstellung ist `1` Stunde (`3600` Sekunden).
- `NoProxy` — Gibt eine durch Leerstellen getrennte Liste von Subnets, IP-Adressen, Domains oder Hosts an, deren Inhalte nicht im Cache gehalten werden. Diese Einstellung ist sehr nützlich für Intranet-Seiten.

10.5.64. `NameVirtualHost`

Wenn Sie namensbasierte virtuelle Hosts einrichten, müssen Sie die Anweisung `NameVirtualHost` für die IP-Adresse verwenden und die Portnummer, falls erforderlich. Die Konfiguration von namensbasierten virtuellen Hosts wird verwendet, wenn Sie verschiedene virtuelle Hosts für verschiedene Domänen einrichten möchten, aber nicht genügend verschiedene IP-Adressen für die verschiedenen Domänennamen haben (oder verwenden möchten), für die Ihr Web-Server Dokumente bereitstellt.

Bitte beachten

Alle eingerichteten namensbasierten virtuellen Hosts funktionieren nur für unverschlüsselte HTTP-Verbindungen, da Sie keine namensbasierten virtuellen Hosts für einen verschlüsselten Server verwenden können. Müssen Sie virtuelle Hosts mit einem verschlüsselten Server verwenden, benötigen Sie IP-adressbasierte virtuelle Hosts.

Wenn Sie namensbasierte virtuelle Hosts verwenden, sind für die Konfigurationsanweisung `NameVirtualHost` die Kommentare zu entfernen, und nach `NameVirtualHost` ist die richtige IP-Adresse für Ihren Server anzugeben. Anschließend sind mit `VirtualHost`-Tags weitere Informationen zu den verschiedenen Domänen hinzuzufügen, die `ServerName` für jeden virtuellen Host sowie weitere Konfigurationsanweisungen einschließen, die nur für diesen virtuellen Host gelten.

10.5.65. `VirtualHost`

<VirtualHost>- und </VirtualHost>-Tags erzeugen einen Container, der die Eigenschaften eines virtuellen Hosts angibt. Der `VirtualHost` Container akzeptiert die meisten Konfigurationsanweisungen.

Eine Reihe von auskommentierten `VirtualHost`-Tags sind in `httpd.conf` enthalten, was die minimalen Konfigurationsanweisungen beschreibt, die für die Einrichtung eines virtuellen Hosts benötigt sind. Weitere Informationen über virtuelle Hosts finden Sie in Abschnitt 10.8.

Bitte beachten

Alle virtuellen Hostumgebungen von SSL wurden in die Datei `/etc/httpd/conf.d/ssl.conf` verschoben.

10.5.66. SSL-Konfigurationsanweisungen

Die Anweisungen in der Datei `/etc/httpd/conf.d/ssl.conf` können so konfiguriert werden, dass sichere Web-Kommunikationen mit SSL und TLS möglich sind.

10.5.66.1. `SetEnvIf`

Die Apache-Konfigurationsanweisung `SetEnvIf` kann dazu verwendet werden, um Umgebungsvariablen zu setzen, die auf Kopfinformationen der Anfrage basieren. In der mitgelieferten Datei `httpd.conf` wird zur Deaktivierung von HTTP-Keepalive verwendet und ermöglicht SSL das Schließen der Verbindung, ohne dass ein Close Notify-Alarm vom Client-Browser gesendet wird. Diese Einstellung ist für bestimmte Browser erforderlich, die die SSL-Verbindung nicht zuverlässig beenden.

Für weitere Informationen zu SSL-Anweisungen rufen Sie mit Ihrem Browser die folgenden Seiten auf:

- http://localhost/manual/mod/mod_ssl.html
- http://httpd.apache.org/docs-2.0/mod/mod_ssl.html

Informationen darüber, wie man einen Apache HTTP Secure Server einrichtet, finden Sie im Kapitel *Apache HTTP Secure Server Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Bitte beachten

Nehmen Sie keine Veränderungen an Ihren SSL-Anweisungen vor, es sei denn, Sie wissen genau, was Sie tun. In den meisten Fällen sind die SSL-Anweisungen in der installierten Form völlig ausreichend.

10.6. Standard-Module

Apache HTTP Server wird mit einer Reihe von Modulen vertrieben. Standardmäßig werden folgende Module mit dem `httpd` Packet auf Red Hat Enterprise Linux 3 installiert und aktiviert:

```
mod_access.so
mod_auth.so
mod_auth_anon.so
mod_auth_dbm.so
mod_auth_digest.so
mod_include.so
mod_log_config.so
mod_env.so
mod_mime_magic.so
mod_cern_meta.so
mod_expires.so
mod_headers.so
mod_usertrack.so
mod_unique_id.so
mod_setenvif.so
mod_mime.so
mod_dav.so
mod_status.so
mod_autoindex.so
mod_asis.so
mod_info.so
mod_dav_fs.so
mod_vhost_alias.so
mod_negotiation.so
mod_dir.so
mod_imap.so
mod_actions.so
mod_speling.so
mod_userdir.so
mod_alias.so
mod_rewrite.so
mod_proxy.so
mod_proxy_ftp.so
mod_proxy_http.so
mod_proxy_connect.so
mod_cache.so
mod_disk_cache.so
mod_file_cache.so
mod_mem_cache.so
mod_cgi.so
```

Folgende Module sind zusätzlich verfügbar, wenn Sie weitere Pakete installieren:

```
mod_auth_mysql
mod_auth_pgsql
mod_perl
mod_python
mod_ssl
php
```

10.7. Hinzufügen von Modulen zu Ihrem Server

Da Apache HTTP Server 2.0 DSOs unterstützt, können Sie Apache Module auf einfache Weise laden bzw. Ihre eigenen Module einkompilieren. DSO-Unterstützung bedeutet auch, dass Module während der Laufzeit dynamisch nach Bedarf geladen werden können und so keinen Speicherplatz auf dem Server belegen.

Das Apache Project stellt eine vollständige DSO-Dokumentation unter http://httpd.apache.org/docs-2.0/dso.html zur Verfügung. Nach der Installation des Pakets `http-manual` können Sie auch unter http://localhost/manual/mod/Dokumentationen zu Apache Modulen finden.

Damit Apache HTTP Server ein DSO-Modul verwenden kann, muss dieses in einer `LoadModule`-Anweisung in der Datei `/etc/httpd/conf/httpd.conf` enthalten sein. Wenn das Modul von einem separaten Paket bereit gestellt wird, muss diese Zeile in der Konfigurationsdatei des Moduls im Verzeichnis `/etc/httpd/conf.d/` erscheinen. Sehen Sie Abschnitt 10.5.12 für weitere Informationen zur `LoadModule`-Anweisung.

Wenn Sie Module aus `http.conf` hinzufügen oder löschen, müssen Sie Apache neu laden oder starten, wie in Abschnitt 10.4 beschrieben.

Wenn Sie ein eigenes Modul haben, können Sie es zur Datei `httpd.conf` hinzufügen, damit es als ein DSO einkompiliert und geladen wird. Dazu müssen Sie das Paket `httpd-devel` installieren, weil es die Include-Dateien, die Header-Dateien und die *APache eXtenSion* (`apxs`) enthält. Der Befehl `apxs` verwendet die Include-Dateien und die Header-Dateien zum Kompilieren der Apache-Module.

Wenn Sie ein eigenes Modul geschrieben haben, sollten Sie `/usr/sbin/apxs` verwenden, um die Modulquellen außerhalb des Apache Quellbaums zu kompilieren. Für weitere Informationen zur Verwendung des Befehls `/usr/sbin/apxs`, sehen Sie die Apache Dokumentation Online unter http://httpd.apache.org/docs-2.0/dso.html und die man-Seiten zu `apxs`.

Speichern Sie Ihr Modul nach dem Kompilieren im Verzeichnis `/usr/lib/httpd/modules/`. Fügen Sie dann der Datei `httpd.conf` eine `LoadModule`-Zeile hinzu, die folgendes Format verwendet:

```
LoadModule <module-name>
<path/to/module.so>
```

Beachten Sie, dass Sie den den Namen von *<foo_module>* und *<mod_foo.so>* in geeigneter Weise ändern müssen.

10.8. Virtuelle Hosts verwenden

Apache HTTP Server bietet die Möglichkeit zur Verwendung von virtuellen Hosts, um verschiedene Server für verschiedene IP-Adressen, verschiedene Rechnernamen oder verschiedene Ports auf demselben Server zu benutzen. Wenn Sie virtuelle Hosts verwenden möchten, so finden Sie detaillierte Informationen in der Apache-Dokumentation oder unter http://httpd.apache.org/docs-2.0/vhosts/.

10.8.1. Einrichten von Virtual Hosts

Um einen Namens-basierten Virtual Host zu erzeugen, ist es am besten den Virtual-Host-Container in `httpd.conf` als Grundlage zu verwenden.

Das Beispiel des Virtual Host liest sich wie folgt:

```
#NameVirtualHost *
#
#<VirtualHost  *>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
```

```
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
```

Um Namens-basiertes Virtual Hosting zu aktivieren, entfernen Sie das Kommentarsymbol (`#`) aus der `NameVirtualHost`-Zeile und ersetzen Sie den Stern (`*`) mit der IP-Adresse, die dem Rechner zugewiesen ist.

Als nächstes, konfigurieren Sie einen Virtual Host, indem Sie die Kommetarsymbole im `<VirtualHost>`-Container entfernen, und die Werte benutzerdefiniert einstellen.

In der `<VirtualHost>`-Zeile, ändern Sie den Stern (`*`) in die IP-Adresse des Servers. Ändern Sie `ServerName` auf einen *gültigen*, dem Rechner zugewiesenen, DNS-Namen und konfigurieren Sie andere Anweisungen entsprechend.

Der `<VirtualHost>`-Container ist in hohem Grade benutzerdefinierbar und akzeptiert nahezu jede Anweisung in der allgemeinen Server-Konfiguration.

Tipp

Wenn Sie einen Virtual Host dazu konfigurieren einen nicht-Standard Port abzuhören, muss dieser Port zur `Listen`-Anweisung in den allgemeinen Einstellungen der Datei `/etc/httpd/conf/http.conf` hinzugefügt werden.

Um einen neu erzeugten Virtual Host zu aktivieren, muss Apache HTTP Server neu geladen oder neu gestartet werden. Sehen Sie Abschnitt 10.4 für diesbezügliche Anleitungen.

Umfassende Informationen zum Erzeugen und Konfigurieren beider, Namens-basierter und IP-basierter Virtual Hosts, finden Sie Online unter http://httpd.apache.org/docs-2.0/vhosts/.

10.8.2. Der virtuelle Host des Secure Web-Servers

In der Standardkonfiguration Ihres Red Hat Enterprise Linux AS wird ein unverschlüsselter und Secure Server ausgeführt. Beide Server verwenden dieselbe IP-Adresse und denselben Host-Namen, warten jedoch an verschiedenen Ports auf Anforderungen. Außerdem ist der sichere Server ein virtueller Host. Mit dieser Konfiguration können Sie sowohl unverschlüsselte als auch verschlüsselte Dokumente bereitstellen. Wie Ihnen wahrscheinlich bekannt ist, erfordern sichere HTTP-Übertragungen mehr Zeit als nicht verschlüsselte Übertragungen, da während der sicheren Transaktionen erheblich mehr Informationen ausgetauscht werden. Die Verwendung Ihres Secure Servers für unverschlüsselten Web-Datenverkehr ist daher nicht zu empfehlen.

Ein Aspekt SSL-unterstützter HTTP-Übertragungen ist, dass diese mehr Ressourcen benötigen als das Standard-HTTP-Protokoll, weswegen ein Secure Server nicht die gleiche Anzahl an Seiten pro Sekunde bereitstellen kann. Aus diesem Grund ist es oft ratsam, die von einem Secure Server bereitgestellte Information zu minimieren, vor allem, wenn die Seite viele Anfragen erhält.

Wichtig

Do not use name-based virtual hosts in conjunction with a secure Web server as the SSL handshake occurs before the HTTP request identifies the appropriate name-based virtual host. Name-based virtual hosts only work with the non-secure Web server.

The configuration directives for the secure server are contained within virtual host tags in the `/etc/httpd/conf.d/ssl.conf` file.

Standardmäßig verwenden sowohl der sichere als auch der unverschlüsselte Web-Server dieselbe `DocumentRoot`. Um `DocumentRoot` so zu ändern, dass es nicht mehr gemeinsam vom sicheren und vom unverschlüsselten Server verwendet wird, ist eine der `DocumentRoot`-Anweisungen zu ändern. Die `DocumentRoot` Anweisung innerhalb oder außerhalb der Virtual Host-Tags in der Datei `httpd.conf` definiert die `DocumentRoot` für Ihren unverschlüsselten Web-Server. Die `DocumentRoot` Anweisung in der Datei `conf.d/ssl.conf` innerhalb der Virtual Host-Tags definiert DocumentRoot für den verschlüsselten Server.

Um nicht-sichere Web-Server vom Akzeptieren einer Verbindung abzuhalten, kommentieren Sie die Zeile `Listen 80` in der Datei `httpd.conf` aus, indem Sie ein Kommentarsymbol ([#]) voranstellen. Die Zeile wird dann wie Folgt aussehen:

```
#Listen 80
```

Für weitere Informationen zum Konfigurieren eines SSL-unterstützten Web-Servers, sehen Sie das Kapitel *Apache HTTP Secure Server Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*. Für weiterführende Hinweise, sehen Sie die Dokumentation der Apache Software Foundation Online unter den folgenden URLs:

- http://httpd.apache.org/docs-2.0/ssl/.
- http://httpd.apache.org/docs-2.0/vhosts/

10.9. Zusätzliche Ressourcen

Weitere Informationen zu Apache HTTP Server finden Sie in folgenden Ressourcen:

10.9.1. Hilfreiche Websites

- http://httpd.apache.org — Die offizielle Website für den Apache HTTP Server Web-Server mit Dokumentationen zu allen Anweisungen und Standardmodulen.
- http://www.modssl.org — Die offizielle Website für `mod_ssl`.
- http://www.apacheweek.com/ — Eine wöchentliche Online-Ausgabe über Alles, was Apache betrifft.

10.9.2. Zusätzliche Bücher

- *Apache Desktop Reference* von Ralf S. Engelschall; Addison Wesley. Verfasst von dem ASF-Mitglied und mod_ssl-Autor Ralf Engelschall, das *Apache Desktop Reference* ist ein kompaktes jedoch all umfassendes Nachschlagewerk zur Verwendung von Apache, Kompilierung, Konfiguration, und Laufzeit. Dieses Buch steht online unter http://www.apacheref.com/ zur Verfügung.
- *Professional Apache* von Peter Wainwright; Wrox Press Ltd. *Professional Apache* stammt von Wrox Press Ltd, und richtet sich sowohl an erfahrene Web-Server-Administratoren als auch an Anfänger.
- *Administering Apache* von Mark Allan Arnold; Osborne Media Group. Dieses Buch ist für Internet-Dienstleistungsanbieter, die sicherere Dienste liefern wollen.
- *Apache Server Unleashed* von Richard Bowen, et al; SAMS BOOKS. Das Buch ist eine Enzyklopädie für Apache.

- *Apache Pocket Reference* von Andrew Ford, Gigi Estabrook; O'Reilly. Dies ist das letzte Werk der Reihe O'Reilly Pocket Reference.
- *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Enthält ein Kapitel zur Konfiguration von Apache HTTP Server, unter Verwendung von **HTTP Configuration Tool** und ein Kapitel zur Konfiguration eines Apache HTTP Server Secure Servers.
- *Red Hat Enterprise Linux Sicherheitshandbuch*; Red Hat, Inc. — Das Kapitel *Server-Sicherheit* beschreibt Wege den Apache HTTP Server und andere Services sicher zu machen.

Kapitel 11.
Berkeley Internet Name Domain (BIND)

Die meisten modernen Netzwerke, einschliesslich dem Internet, erlauben dem Benutzer andere Computer über deren Namen zu bestimmen. Dies befreit den Benutzer davon, die numerische Netzwerk-Adresse behalten zu müssen. Der effektivste Weg ein Netzwerk zu konfigurieren, sodass es namensbasierte Verbindungen zulässt, ist durch das Einrichten eines *Domain Name Service* (*DNS*) oder *Nameserver*, welcher Rechnernamen in numerische Adressen auflöst und umgekehrt.

Dieses Kapitel stellt den in Red Hat Enterprise Linux enthaltenen Nameserver, *Berkeley Internet Name Domain* (*BIND*) DNS Server, vor, mit dem Fokus auf die Struktur dessen Konfigurationsdateien und der Art und Weise, wie dieser lokal und auch remote verwaltet werden kann.

Anweisungen für die Konfiguration von BIND unter Verwendung des graphischen **Domain Name Service Configuration Tool** (`redhat-config-bind`) finden Sie im Kapitel *BIND-Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Warnung

Wenn Sie das **Domain Name Service Configuration Tool** verwenden, sollten Sie die BIND-Konfigurationsdateien nicht manuell bearbeiten, da alle manuell vorgenommenen Änderungen vom **Domain Name Service Configuration Tool** überschrieben werden.

11.1. Einführung in den DNS

Wenn Hosts auf einem Netzwerk zu einem anderen über deren Hostnamen, auch *fully qualified domain name (FQDN)* genannt, verbinden, wird DNS verwendet, um die IP-Adressen der Rechner über deren Hostnamen zu bestimmen.

Die Verwendung von DNS und FQDN sind auch für Systemadministratoren vorteilhaft. Dank dieser Namen verfügen Administratoren über die Flexibilität, IP-Adressen für einzelne Rechner zu ändern, ohne namenbasierte Abfragen der Rechner ausführen zu müssen. Umgekehrt können die Administratoren festlegen, welche Rechner eine namenbasierte Abfrage in einer für die Benutzer transparenten Weise handhaben.

DNS wird im Allgemeinen mit Hilfe zentralisierter Server implementiert, die für einige Domains authorisiert sind und sich auf andere DNS-Server für andere Domains beziehen.

Eine Client-Applikation verbindet üblicherweise über den Port 53 mit dem Nameserver und fragt Informationen über diesen ab. Der Nameserver wird versuchen, mit Hilfe einer Resolver-Bibliothek den FQDN zu lösen. Diese Bibliothek kann die vom Host angeforderten Informationen oder Daten über den Namen aus einer früheren Abfrage enthalten. Wenn der Nameserver die Antwort nicht in seiner Resolver-Bibliothek findet, wird er andere Nameserver, die sogenannten *Root- Nameserver* verwenden, um festzulegen, welche Nameserver für diesen FQDN autorisiert sind. Mit dieser Information wird anschließend bei den autorisierten Nameservern dieser Name abgefragt, um die IP-Adresse festzustellen. Bei einem Reverse-Lookup wird die gleiche Prozedur durchgeführt, allerdings mit dem Unterschied, dass hier eine unbekannte IP-Adresse und nicht ein Name abgefragt wird.

11.1.1. Nameserver Zonen

Im Internet kann ein FQDN eines Hosts in verschiedene Bereiche eingeteilt werden. Diese Bereiche werden in einer Hierarchie (ähnlich einem Baum) mit Hauptstamm, primären Abzweigungen, sekundären Abzweigungen usw. angeordnet. Betrachten Sie den folgenden FQDN:

```
bob.sales.example.com
```

Wenn Sie sehen möchten, wie ein FQDN aufgelöst wurde, um eine IP-Adresse für ein bestimmtes System zu finden, müssen Sie den Namen von rechts nach links lesen. Jede Ebene der Hierarchie ist durch Punkte (`.`) voneinander getrennt. In diesem Beispiel bestimmt `com` die *Top-Level-Domain* für diesen FQDN. Der `domain`-Name ist eine Subdomain von `com` mit `sales` als Subdomain von `example`. Ganz links im FQDN befindet sich der Hostname, `bob`, der einen bestimmten Computer identifiziert.

Mit Ausnahme des Hostnamens wird jeder Bereich als *Zone* bezeichnet, die einen bestimmten *Namespace* (Namensbereich) festlegt. Ein Namespace kontrolliert die Bezeichnung der Subdomains auf der linken Seite. In diesem Beispiel sind zwar nur zwei Subdomains angegeben, ein FQDN muss aber mindestens eine und kann viel mehr Subdomains enthalten, je nach der Organisation des Namespace.

Die Zonen werden mit Hilfe von *Zone-Dateien* in authorisierten Nameservern festgelegt. Die Zone-Dateien beschreiben den Namenspace der Zone, den für eine bestimmte Domain oder Subdomain zu verwendenden Mail-Server, uvm. Die Zone-Dateien sind auf *primären Nameservern* (auch *Master-Nameserver* genannt) gespeichert, die für Änderungen an Dateien maßgeblich sind, sowie auf *sekundären Nameservern* (auch *Slave-Nameserver* genannt), die ihre Zone-Dateien von den primären Nameservern erhalten. Jeder Nameserver kann gleichzeitig für unterschiedliche Zonen sowohl primärer als auch sekundärer Nameserver sein. Zugleich können sie auch für mehrere Zonen maßgeblich sein. Dies hängt alles von der Konfiguration des Nameservers ab.

11.1.2. Nameserver Types

Primäre Nameserver können auf vier verschiedene Arten konfiguriert sein:

- *Master* — Speichert die ursprünglichen und maßgeblichen Zonen für einen bestimmten Namespace, und beantwortet Fragen von anderen Nameservern, die nach Antworten für diesen Namespace suchen.
- *Slave* — Beantwortet ebenfalls die Anfragen anderer Nameserver bezüglich des Namespace, für den dieser die Autorität darstellt. Die Slave-Nameserver erhalten ihre Informationen über ein Namespace jedoch von Master-Nameservern.
- *Caching-Only* — Bietet Services für IP-Auflösungen, hat aber nicht für alle Zonen eine Berechtigung. Antworten für alle Auflösungen werden üblicherweise in einer Datenbank bearbeitet, die für eine bestimmte Zeit im Hauptspeicher verbleibt. Sie werden von dem Zone-Record, das die Antworten erhält, nach der ersten Auflösung für andere DNS-Clients festgelegt.
- *Forwarding* — Leitet Anfragen zum Auflösen an eine spezielle Liste von Nameservern weiter. Wenn keiner der angegebenen Nameserver den Auflösungsprozess durchführen kann, wird der Vorgang abgebrochen und die Auflösung schlägt fehl.

Ein Nameserver kann einem oder mehreren dieser Typen zugehören. Zum Beispiel kann ein Nameserver für einige Zonen der Master und für andere Zonen der Slave sein und für andere ausschließlich Auflösungen weiterleiten.

11.1.3. BIND als Nameserver

BIND führt Namensauflösungsdienste mittles des `/usr/sbin/named` Daemon durch. BIND enthält auch ein administratives Utility, `/usr/sbin/rndc` genannt. Mehr Information zu `rndc` kann unter Abschnitt 11.4 gefunden werden.

BIND speichert seine Konfigurationsdateien in den folgenden zwei Orten:

- `/etc/named.conf` — Die Konfigurationsdatei für den `named` Daemon.

- `/var/named/` directory — Das `named` Arbeitsverzeichnis, welches Zone, Statistiken, und Cache-Dateien enthält.

Die nächsten zwei Abschnitte behandeln die BIND Konfigurationsdateien in mehr Detail.

11.2. `/etc/named.conf`

Die `/etc/named.conf`-Datei ist eine Ansammlung von Direktiven, die in verschachtelte, geschweifte Klammern platzierte `{ }`-Optionen verwenden. Administratoren müssen vorsichtig beim Bearbeiten der Datei `named.conf` sein und jegliche syntaktische Fehler veremeiden, da auch die kleinsten Fehler den Service `named` vom Starten abhalten können.

Warnung

Bearbeiten Sie die Datei `/etc/named.conf` oder andere Dateien aus dem `/var/named/`-Verzeichnis *nicht* manuell, wenn Sie mit dem **Domain Name Service Configuration Tool** arbeiten. Alle manuell vorgenommenen Änderungen an diese Dateien werden überschrieben, wenn **Domain Name Service Configuration Tool** das nächste Mal verwendet wird.

Eine typische `named.conf`-Datei ist ähnlich wie folgt gegliedert:

```
<statement-1> ["<statement-1-name>"] [<statement-1-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};

<statement-2> ["<statement-2-name>"] [<statement-2-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};

<statement-N> ["<statement-N-name>"] [<statement-N-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};
```

11.2.1. Häufig verwendete Typen von Statements

Die folgenden Typen von Statements werden häufig in `/etc/named.conf` verwendet:

11.2.1.1. `acl` Statement

Das `acl` Statement (Access Control Statement) definiert eine Gruppe von Hosts, welchen Zugriff zum Nameserver erlaubt oder verboten werden kann.

Ein `acl` Statement hat folgende Form:

```
acl <acl-name> {
    <match-element>;
    [<match-element>; ...]
};
```

In diesem Statement ersetzen Sie *<acl-name>* mit dem Namen der Access-Control-List (Liste der Zugriffskontrolle) und ersetzen Sie *<match-element>* mit einer List von IP-Adressen, wobei Adressen durch ein Semikolon getrennt werden. Meistens wird eine individuelle IP-Adresse oder IP-Netzwerk-Notation (wie `10.0.1.0/24`) benutzt, um die IP Adresse im `acl` Statement zu identifizieren.

Die folgenden Access-Control-Lists sind bereits als Schlüsselwörter definiert, um die Konfiguration zu vereinfachen:

- `any` — Vergleicht jede IP-Adresse.
- `localhost` — Vergleicht jede IP-Adresse, die auf dem lokalen System verwendet wird.
- `localnets` — Vergleicht jede IP-Adresse auf allen Netzwerken, mit denen das lokale System verbunden ist.
- `none` — Vergleicht keine IP-Adressen.

Wenn mit anderen Statements (wie dem `options` Statement) verwendet, können `acl` Statements sehr hilfreich dabei sein, BIND Nameserver vor unbefugtem Zugriff zu schützen.

Das folgende Beispiel gibt zwei Access-Control-Lists und benutzt ein `options` Statement, um anzugeben, wie diese vom Nameserver behandelt werden sollen:

```
 acl black-hats {
    10.0.2.0/24;
    192.168.0.0/24;
 };

acl red-hats {
    10.0.1.0/24;
 };

options {
    blackhole { black-hats; };
    allow-query { red-hats; };
    allow-recursion { red-hats; };
 }
```

Dieses Beispiel enthält zwei Access-Control-Lists, `black-hats` und `red-hats`. Hosts in der `black-hats` Liste ist der Zugriff zum Nameserver verboten, während Hosts in der `red-hats` Liste normaler Zugriff gewährt ist.

11.2.1.2. `include` Statement

Das `include` Statement erlaubt Dateien in `named.conf` einzuschliessen. In dieser Weise können sensitive Konfigurationsdaten (wie `keys`) in einer separaten Datei mit eingeschränkten Rechten gehalten werden.

Ein `include` Statement hat die folgende Form:

```
include  "<file-name>"
```

In diesem Statement, ersetzen Sie *<file-name>* mit dem absoluten Pfad zu einer Datei.

11.2.1.3. `options` Statement

Das `options` Statement legt Konfigurationsoptionen des globalen Servers fest und setzt Defaults für andere Statements. Es kann verwendet werden, um den Ort des `named` Arbeitsverzeichnisses anzugeben, den Typ der erlaubten Queries, uvm.

Das `options` Statement hat die folgende Form:

```
options {
        <option>;
 [<option>; ...]
};
```

In diesem Statement, ersetzen Sie die *<option>* Direktiven mit einer gültigen Option.

Die folgenden sind häufig benutzte Optionen:

- `allow-query` — Legt fest, welche Hosts diesen Nameserver abfragen dürfen. Standardmäßig sind alle Hosts dazu berechtigt. Mit Hilfe einer Access-Controll-List, einer Sammlung von IP-Adressen oder Netzwerken kann festgelegt werden, dass nur bestimmte Hosts den Nameserver abfragen dürfen.
- `allow-recursion` — Ähnelt der Option `allow-query`, mit der Ausnahme, dass sie sich auf rekursive Abfragen bezieht. Standardmäßig können alle Hosts rekursive Abfragen auf dem Nameserver durchführen.
- `blackhole` — Gibt an, welchen Hosts es nicht erlaubt is Anfragen an den Server zu stellen.
- `directory` — Ändert das `named`-Arbeitsverzeichnis, so dass es sich von dem Default, `/var/named/`, unterscheidet.
- `forward` — Kontrolliert das Verhalten beim Weiterleiten einer `forwarders` Direktive.

  Die folgenden Optionen werden angenommen:

  - `first` — Gibt an, dass Nameserver, die in der `forwarders`-Option festgelegt sind, zuerst nach Informationen abgefragt werden. Sollten anschließend keine Informationen vorhanden sein, versucht `named` die Auflösung selbst durchzuführen.
  - `only` — Gibt an, dass `named` nicht versucht die Auflösung selbst durchzuführen, wenn die `forwarders` Direktive nicht erfolgreich war.

- `forwarders` — Legt eine Liste von Nameservern fest, bei denen Abfragen für Auflösungen weitergeleitet werden.
- `listen-on` — Legt die Netzwerk-Schnittstelle fest, die `named` verwendet, um Anfragen zu prüfen. Standardmäßig werden alle Schnittstellen verwendet.

  Auf diese Weise, sollte der DNS Server auch der Gateway sein, kann BIND dazu konfiguriert werden nur Anfragen, welche von einem dieser Netzwerke gestellt wurden, zu beantworten.

  Eine `listen-on` Direktive kann folgendermaßen aussehen:

  ```
  options {
     listen-on { 10.0.1.1; };
  };
  ```

  Auf diese Art und Weise werden nur Anfragen von der Netzwerk-Schnittstelle akzeptiert, die das private Netzwerk (`10.0.1.1`) verwendet.
- `notify` — Wird verwendet, wenn die Zone als Slave `type` festgelegt ist. Die `masters`- Option teilt dem `named` eines Slaves die IP-Adressen mit, von denen maßgebliche Informationen über die Zone angefragt werden:

  - `yes` — Informiert Slave-Server.

- `no` — Informiert Slave-Server nicht.
- `explicit` — Informiert Slave-Server nur dann, wenn diese in einer `also-notify` List innerhalb des Zonen Statement angegeben sind.

- `pid-file` — Erlaubt das Festlegen eines alternativen Ortes für die Prozess-ID-Datei, die `named` erstellt.
- `statistics-file` — Erlaubt das Festlegen eines alternativen Ortes in welcher die Statistik-Dateien abgelegt werden. Standardmäßig werden `named`-Statistiken in `/var/named/named.stats` gespeichert.

Es gibt noch zahlreiche andere Optionen, bei denen einige voneinander abhängig sind, um fehlerfrei zu funktionieren. Weitere Informationen hierzu finden Sie im *BIND 9 Administrator Reference Manual*, in Abschnitt 11.7.1, und in den man-Seiten zu `bind.conf`.

11.2.1.4. `zone` Statement

Ein `zone` Statement legt die Eigenschaften einer Zone, wie den Ort der Konfigurationsdatei und Zonen-spezifische Optionen fest. Diese Statement kann benutzt werden um globale `options` Statements zu überschreiben.

Ein `zone` Statement hat die folgende Form:

```
zone <zone-name> <zone-class> {
     <zone-options>;
     [<zone-options>; ...]
};
```

In diesem Statement *<zone-name>* ist der Name der Zone, *<zone-class>* ist die optionale Klasse der Zone, und *<zone-options>* ist eine List von Optionen, welche die Eigenschaften der Zone bestimmen.

Das *<zone-name>*-Attribut für die Zone ist besonders wichtig, da es den Standardwert für die `$ORIGIN` Direktive festlegt, welche den Zonen-Dateien im Verzeichnis `/var/named/` entspricht. Der `named` Daemon hängt den Namen der Zone an jeden nicht-FQDN an, welcher in der Zonen-Datei aufgelistet ist.

Wenn, zum Beispiel, ein `zone` Statement den Namespace für `example.com` angibt, verwende `example.com` als *<zone-name>*, damit es an Hostnamen in der `example.com` Zonen-Datei angehängt wird.

Für mehr Information zu Zonen-Dateien, siehe Abschnitt 11.3.

Die am häufigsten verwendeten Optionen von `zone` Statement sind die Folgenden:

- `allow-query` — Legt fest, welche Clients Informationen über diese Zone anfordern dürfen. Standardmäßig sind alle Anfragen zulässig.
- `allow-transfer` — Bestimmt die Slave-Server, die den Transfer der Informationen über die Zonen anfordern dürfen. Standardmäßig sind alle Transfer-Anfragen zulässig.
- `allow-update` — Bestimmt die Hosts, die Informationen in ihrer Zone dynamisch aktualisieren dürfen. Standardmäßig sind Anfragen für dynamische Updates nicht zulässig.

  Wenn Sie zulassen, dass Hosts Informationen über ihre Zonen aktualisieren, sollten Sie unbedingt sicherstellen, dass Sie diese Option nur aktivieren, wenn der Host absolut sicher ist. Es ist besser, die Updates der Zonen-Records manuell von einem Administrator durchführen zu lassen und den `named`-Service, soweit möglich, neu zu laden.

- `file` — Bestimmt den Namen der Datei im `named`-Arbeitsverzeichnis, die die Zone-Konfigurationsdateien enthält. Standardmäßig ist dies `/var/named/`.
- `masters` — Gibt die IP-Adressen an, von denen authoritäre Zoneninformationen erfragt werden können. Wird nur verwendet, wenn die Zone als `type slave` spezifiziert ist.
- `notify` — Gibt an, ob `named` den Slave-Servern mitteilt, daß eine Zone geändert wurde. Diese Direktive kennt die folgenden Optionen:
  - `yes` — Informiert Slave-Server.
  - `no` — Informiert Slave-Server nicht.
  - `explicit` — Informiert Slave-Server nur dann, wenn diese in einer `also-notify` List innerhalb des Zonen Statement angegeben sind.

- `type` — Gibt den Typ der Zone an.

  Folgend ist eine Liste der gültigen Optionen:
  - `forward` — Weist den Nameserver an, alle Anfragen zu Informationen über die Zone an andere Nameserver weiterzuleiten.
  - `hint` — Ein spezieller Zonen-Typ, mit dem auf die Root-Nameserver verwiesen wird, die verwendet werden, um Abfragen zu lösen, wenn eine Zone ansonsten unbekannt ist. Sie brauchen neben der Standarddatei `/etc/named.conf` keine zusätzliche Hinweisdatei konfigurieren.
  - `master` — Bezeichnet den Nameserver, der für diese Zone maßgeblich ist. Wenn die Konfigurationsdateien für diese Zone auf Ihrem System sind, sollte der `master`-Typ eingestellt werden.
  - `slave` — Bezeichnet den Nameserver, der für diese Zone der Slave-Server ist und der `named` mitteilt, die Zonen-Konfigurationsdateien für diese Zone von der IP-Adresse des Master-Nameservers abzufragen.

- `zone-statistics` — Weist `named` an, die Statistiken über diese Zone aufzubewahren und diese entweder in der Standard-Datei (`/var/named/named.stats`) oder an einer Stelle abzulegen, die mit der `statistics-file`-Option in der `server`-Anweisung, sofern vorhanden, dafür eingerichtet wurde. Sehen Sie Abschnitt 11.2.2 für mehr Information über das `server` Statement.

11.2.1.5. Beispiele von `zone`-Statements

Die meisten Änderungen in der `/etc/named.conf`-Datei eines Master- oder Slave-Nameservers betreffen das Hinzufügen, Modifizieren oder Löschen von `zone`-Direktiven. Obwohl diese `zone`-Anweisungen mehrere Optionen enthalten können, werden von den meisten Nameservern nur wenige verwendet. Die folgenden `zone`-Direktiven sind sehr allgemeine Beispiele, die auf Master-Slave-Nameservern verwendet werden können.

Nachfolgend finden Sie ein Beispiel für eine `zone`- Anweisung für den primären Nameserver, der `example.com` (`192.168.0.1`) hostet:

```
zone "example.com" IN {
  type master;
  file "example.com.zone";
  allow-update { none; };
};
```

Diese `zone`-Direktive benennt die Zone `example.com`, stellt als Typ `master` ein und weist den `named`-Service an, die Datei `/var/named/example.com.zone` zu lesen und weist `named` an, Aktualisierungen durch andere Hosts nicht zuzulassen.

Eine zone-Anweisung eines Slave-Servers für example.com unterscheidet sich etwas vom vorherigen Beispiel. Für einen Slave-Server wird der Typ auf slave festgelegt. An die Stelle der Zeile allow-update tritt eine Anweisung, die named die IP-Adresse des Master-Servers mitteilt.

Nachfolgend finden Sie ein Beispiel für eine zone-Anweisung für die example.com Zone:

```
zone "example.com" {
  type slave;
  file "example.com.zone";
  masters { 192.168.0.1; };
};
```

Diese zone-Anweisung weist named auf dem Slave-Server an, bei dem Master-Server mit der IP 192.168.0.1 nach Informationen für die Zone example.com zu suchen. Die Informationen, die der Slave-Server vom Master-Server erhält, werden in der Datei /var/named/example.com.zone gespeichert.

11.2.2. Andere Statement-Typen

Die Folgende ist eine Liste von weniger verwendeten Statement-Typen welche in named.conf verfügbar sind:

- controls — Konfiguriert verschiedene Sicherheitsbedingungen, die für den Befehl rndc zum Verwalten des named-Services nötig sind.

  Unter Abschnitt 11.4.1 sehen Sie, wie die controls-Anweisung aussehen sollte, einschließlich der verfügbaren Optionen.

- key "<*key-name*>" — Legt für einen bestimmten Schlüssel einen Namen fest. Schlüssel werden verwendet, um verschiedene Aktionen zu authentifizieren, wie z.B. sichere Updates oder die Verwendung des rndc-Befehls. Mit key werden zwei Optionen verwendet:

  - algorithm <*algorithm-name*> — Der verwendete Algorithmus-Typ, z.B. dsa oder hmac-md5.
  - secret "<*key-value*>" — Der verschlüsselte Schlüssel.

  Unter Abschnitt 11.4.2 finden Sie die Anweisungen zum Schreiben einer key-Direktive.

- logging — Erlaubt die Verwendung mehrerer Arten von Protokollen mit der Bezeichnung *channels*. Wird die Option channel in der logging-Anweisung verwendet, wird ein benutzerdefiniertes Protokoll mit eigenem Dateinamen (file), Größenbeschränkung (size), Version (version), und dessen Wichtigkeit (severity) erstellt. Nachdem ein benutzerdefinierter Channel festgelegt wurde, wird dieser mit der Option category klassifiziert und beginnt mit dem Protokollieren, wenn named neu gestartet wird.

  Standardmäßig protokolliert named normale Mitteilungen im syslog-Daemon, der diese in /var/log/messages platziert. Dies geschieht, weil sich verschiedene standardmäßige Channel mit unterschiedlicher Wichtigkeit im BIND befinden. Zum Beispiel verarbeitet ein Channel die Protokoll-Mitteilungen (default_syslog) und ein anderer speziell Debugging-Mitteilungen (default_debug). Die standardmäßige Kategorie default, verwendet zum normalen Protokollieren, ohne spezielle Konfigurationen, integrierte Channel.

  Den Protokollierungsprozess individuell anzupassen kann sehr aufwendig sein und übersteigt den Umfang dieses Kapitels. Informationen über die Erstellung von benutzerdefinierten BIND-Protokollen finden Sie im *BIND 9 Administrator Reference Manual* in Abschnitt 11.7.1.

- server — Definiert bestimmte Optionen, die Auswirkungen darauf haben, wie named sich gegenüber Remote-Name-Servern verhalten soll, insbesondere im Hinblick auf Benachrichtigungen und Zone-Übertragungen.

Die Option `transfer-format` kontrolliert, ob mit jeder Mitteilung ein Resource-Record (`one-answer`) oder mehrere Ressource-Records mit jeder Meldung gesendet werden (`many-answers`). Da `many-answers` leistungsfähiger ist, wird es nur von neueren Name-Servern angenommen.

- `trusted-keys` — Enthält verschiedene öffentliche Schlüssel für die Verwendung mit Secure DNS (DNSSEC). Unter Abschnitt 11.5.3 finden Sie eine Einführung in die BIND-Sicherheit.
- `view "<view-name>"` — Erstellt spezielle Ansichten, die bestimmten Informationen entsprechen, die von dem Host abhängig sind, der den Name-Server kontaktiert. Dadurch erhalten einige Hosts Informationen, die sich vollkommen von denen unterscheiden, die andere Hosts erhalten. Eine andere Möglichkeit ist, nur bestimmte Zonen für bestimmte sichere Hosts zugänglich zu machen, während nicht sichere Hosts nur Abfragen für andere Zonen erstellen können.

  Es können auch mehrere Ansichten verwendet werden, solange ihre Namen eindeutig sind. Die `match-clients`-Option legt die IP-Adressen fest, die für eine bestimmte Ansicht verwendet werden. Alle `option`-Direktiven können in einer Ansicht verwendet werden. Sie überschreiben dabei die allgemeinen, bereits für `named` konfigurierten Optionen. Die meisten `view`-Direktiven enthalten mehrere `zone`-Anweisungen, die für die `match-clients`-Liste gelten. Es ist wichtig, in welcher Reihenfolge die `view`-Anweisungen aufgelistet sind, da die erste `view`-Direktive, die mit einer bestimmten IP-Adresse des Client übereinstimmt, verwendet wird.

  Unter Abschnitt 11.5.2 finden Sie weitere Informationen zur `view`-Anweisung.

11.2.3. Kommentar-Tags

Die Folgende ist eine Liste gültiger, in `named.conf` verwendeter, Kommentar-Tags:

- `//` — Wenn an den Anfang der Zeile gestellt, wird diese Zeile von `named` ignoriert.
- `#` — Wenn an den Anfang der Zeile gestellt, wird diese Zeile von `named` ignoriert.
- `/*` und `*/` — Hierin eingeschlossener Text wird von `named` ignoriert.

11.3. Zone-Dateien

Zone-Dateien sind im `named`-Arbeitsverzeichnis, `/var/named/`, gespeichert und enthalten Informationen über einen bestimmten Namespace. Jede Zone-Datei ist gemäß der Daten der `file`-Option in der `zone`-Direktive benannt. Normalerweise bezieht sich der Name auf die entsprechende Domain und identifiziert die Datei als Datei, die Zone-Daten enthält, wie z.B. `example.com.zone`.

Jede Zone-Datei kann Direktiven und Resource-Records enthalten. *Direktiven* weisen den Name-Server an, bestimmte Aktionen auszuführen oder spezielle Einstellungen für die Zone zu verwenden. *Resource-Records* legen die Parameter der Zone fest. Diese ordnen bestimmten Systemen innerhalb des Namespaces der Zone eine Identität zu. Anweisungen sind optional, aber Resource-Records sind notwendig, um dieser Zone den Name-Service zur Verfügung zu stellen.

Alle Direktiven und Resource-Records sollten in einer eigenen Zeile stehen.

Kommentare können in Zone-Dateien nach dem Semikolon (`;`) platziert werden.

11.3.1. Zone-Dateien-Direktiven

Anweisungen werden durch das vorangestellte Dollarzeichen `$` identifiziert, das vor dem Namen der Anweisung üblicherweise im oberen Teil der Zone-Datei steht.

Folgende Anweisungen werden am häufigsten verwendet:

- `$INCLUDE` — Weist `named` an, in diese Zone-Datei an Stelle der Anweisung eine andere Zone-Datei einzufügen. Dadurch können zusätzliche Einstellungen der Zone getrennt von der Haupt-Zone-Datei gespeichert werden.
- `$ORIGIN` — Stellt den Domain-Name so ein, dass er an alle ungeeigneten Records angefügt wird. Wie z.B. die, die ausschließlich den Host festlegen.

  Eine Zone-Datei kann z.B. folgende Zeile enthalten:
  ```
  $ORIGIN example.com
  ```
  Jetzt würde an alle Namen, die in Resource-Records verwendet werden und nicht mit einem Punkt (`.`) enden, `example.com` angehängt.

  Anmerkung

  Die Verwendung der `$ORIGIN`-Direktive ist nicht erforderlich, wenn der Name der Zone in `/etc/named.conf` mit dem Wert übereinstimmt, den Sie `$ORIGIN` zuweisen würden. Standardmäßig wird der Name der Zone als Wert der `$ORIGIN`-Anweisung verwendet.

- `$TTL` — Legt den Standard-*Time to Live (TTL)*-Wert für die Zone fest. Dieser Wert legt für die Name-Server in Sekunden fest, wie lange das Resource-Record für die Zone gültig ist. Ein Resource- Record kann einen eigenen TTL-Wert besitzen, der den Wert dieser Anweisung für die Zone überschreibt.

  Wird dieser Wert erhöht, können die Remote-Name-Server die Zone-Informationen länger verarbeiten. Dadurch werden zwar die Abfragen für diese Zone reduziert, es vergrößert sich jedoch der Zeitraum, bis man von den Änderungen der Resource-Records profitieren kann.

11.3.2. Resource-Records der Zone-Datei

Die Hauptkomponente einer Zone-Datei ist deren Resource-Records.

Es gibt viele Typen von Resource-Records, Folgende werden am häufigsten verwendet:

- `A` — Adressen-Record, das einem Namen eine IP-Adresse zuweist. Beispiel:
  ```
  <host>      IN      A      <IP-address>
  ```
  Wenn der `<host>`-Wert nicht angegeben wird, verweist ein `A`-Record auf eine standardmäßige IP-Adresse für den oberen Teil des Namespaces. Dieses System gilt für alle nicht-FQDN-Anfragen.

  Beachten Sie das folgende `A`-Record-Beispiel für die `example.com` Zone-Datei:
  ```
                IN      A       10.0.1.3
  server1       IN      A       10.0.1.5
  ```
  Anfragen für `example.com` richten sich an 10.0.1.3, während Anfragen für `server1.example.com` sich an 10.0.1.5 richten.
- `CNAME` — Name-Record, welcher Namen untereinander zuordnet. Dieser Typ ist auch als Alias bekannt.

  Im nächsten Beispiel wird `named` angewiesen, dass alle Anfragen, die an den `<alias-name>` gesendet werden, auf den Host `<real-name>` zeigen. `CNAME`-Records werden am häufigsten verwendet, um auf Dienste zu verweisen, die ein allgemeines Namensschema für den korrekten Host, wie `www` für Web-Server, verwenden.
  ```
  <alias-name>      IN      CNAME       <real-name>
  ```
  Betrachten Sie das folgende Beispiel. In dieser Einrichtung bindet der `A`-Record einen Hostnamen an eine IP-Adresse, während ein `CNAME`-Record den allgemein verwendeten Hostnamen `www` zuweist.
  ```
  server1       IN      A       10.0.1.5
  ```

```
www             IN      CNAME   server1
```

- MX — Mail eXchange- Record, das angibt, welchen Weg eine Mail nimmt, die an ein bestimmtes Namespace gesendet und von dieser Zone kontrolliert wurde.

  ```
        IN      MX      <preference-value>   <email-server-name>
  ```

  In diesem Beispiel ermöglicht <*preference-value*>, die E-Mail-Server der Reihenfolge nach zu nummerieren, auf denen Sie für dieses Namespace bestimmte E-Mails empfangen möchten, indem Sie einigen E-Mail-Systemen den Vorrang vor anderen geben. Der MX-Resource-Record mit dem niedrigsten <*preference-value*> wird den anderen vorgezogen. Sie können mehreren E-Mail-Servern denselben Wert zuweisen, um den E-Mail-Verkehr zwischen den Servern zu verteilen.

  Der <*email-server-name*> kann ein Hostname oder ein FQDN sein.

  ```
        IN      MX      10      mail.example.com.
        IN      MX      20      mail2.example.com.
  ```

  In diesem Beispiel wird der erste `mail.example.com`-E-Mail-Server vor dem `mail2.example.com`-E-Mail-Server bevorzugt, wenn eine E-Mail für die Domain `example.com` ankommt.

- NS — Name-Server-Record, der die maßgeblichen Name-Server für eine bestimmte Zone anzeigt.

  Beispiel für einen NS-Record:

  ```
        IN      NS      <nameserver-name>
  ```

  Der <*nameserver-name*> sollte ein FQDN sein.

  Anschließend werden zwei Nameserver als maßgeblich für die Domain aufgelistet. Es ist nicht so wichtig, ob diese Namenserver Slave- oder Master-Nameserver sind, da beide bereits maßgebend sind.

  ```
        IN      NS      dns1.example.com.
        IN      NS      dns2.example.com.
  ```

- PTR — PoinTeR-Record verweist auf einen anderen Teil des Namespace.

  PTR-Records werden primär für eine umgekehrte Namensauflösung verwendet, da sie IP-Adressen zu einem bestimmten Namen verweisen. Unter Abschnitt 11.3.4 finden Sie weitere Beispiele zur Verwendung von PTR-Records.

- SOA — Start Of Authority-Record, gibt wichtige maßgebliche Informationen über den Namespace an den Name-Server.

  Nach den Direktiven festgelegt ist ein SOA-Resource-Record, der erste Resource-Record in einer Zone-Datei.

  Das folgende Beispiel zeigt die Basisstruktur eines SOA-Resource-Record:

  ```
  @       IN      SOA     <primary-name-server>      <hostmaster-email>  (
                          <serial-number>
                          <time-to-refresh>
                          <time-to-retry>
                          <time-to-expire>
                          <minimum-TTL>  )
  ```

  Das @-Symbol richtet die $ORIGIN-Anweisung (oder den Namen der Zone, falls die $ORIGIN-Direktive nicht eingestellt ist) als Namespace ein, das von diesem SOA-Resource-Record eingestellt wurde. Als <*primary-Nameserver*> wird der erste, für diese Domain maßgebliche Name-Server verwendet und die E-Mail der über diesen Namespace zu kontaktierenden Person wird durch die <*hostmaster-email*> ersetzt.

  Die <*serial-number*> wird bei jeder Änderung der Zone-Datei erhöht, so dass named erkennt, dass diese Zone neu geladen werden kann. Die <*time-to-refresh*> teilt den Slave-Servern mit, wie lange sie warten müssen, bevor sie beim Master-Nameserver anfragen, ob alle Änderungen für die Zone durchgeführt wurden. Der Wert der <*serial-number*> wird vom

Slave-Server verwendet, um festzustellen, ob veraltete Daten der Zone verwendet werden, die aktualisiert werden sollten.

Die *<time-to-retry>* gibt den Zeitraum an, nach dem eine neue Anfrage bezüglich der Aktualisierung durchgeführt werden soll, wenn der Master-Nameserver auf die letzte Anfrage nicht reagiert hat. Wenn der Master-Nameserver nicht geantwortet hat, bevor die *<time-to-expire>* abläuft, reagiert der Slave-Nameserver nicht mehr auf Anfragen bezüglich des Namespaces.

<minimum-TTL> ist die Zeit, die anderen Nameservern zum Verarbeiten der Zonen-Informationen mindestens zur Verfügung steht.

In BIND werden alle Zeiten in Sekunden angegeben. Sie können jedoch auch Abkürzungen für andere Zeiteinheiten verwenden, wie z.B. Minuten (`M`), Stunden (`H`), Tage (`D`) und Wochen (`W`). In der Tabelle unter Tabelle 11-1 finden Sie Zeiträume in Sekunden und die entsprechende Zeit in anderen Formaten.

Sekunden	Andere Zeiteinheiten
60	1M
1800	30M
3600	1H
10800	3H
21600	6H
43200	12H
86400	1D
259200	3D
604800	1W
31536000	365D

Tabelle 11-1. Sekunden im Vergleich zu anderen Zeiteinheiten

Das folgende Beispiel zeigt Ihnen, wie ein `SOA`-Resource-Record aussehen könnte, wenn es mit echten Werten konfiguriert ist.

```
@     IN     SOA    dns1.example.com.     hostmaster.example.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expire after 1 week
                    86400 )    ; minimum TTL of 1 day
```

11.3.3. Beispiele für Zone-Dateien

Einzeln betrachtet könnten die Anweisungen und Resource-Records schwer zu verstehen sein. Sind beide in einer gemeinsamen Datei plaziert, wird es einfacher.

Im nächsten Beispiel ist eine sehr einfache Zone-Datei abgebildet.

```
$ORIGIN example.com
$TTL 86400
@     IN     SOA    dns1.example.com.     hostmaster.example.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
```

```
                    3600       ; retry after 1 hour
                    604800     ; expire after 1 week
                    86400 )    ; minimum TTL of 1 day

      IN     NS     dns1.example.com.
      IN     NS     dns2.example.com.

      IN     MX     10     mail.example.com.
      IN     MX     20     mail2.example.com.

             IN     A       10.0.1.5

server1      IN     A       10.0.1.5
server2      IN     A       10.0.1.7
dns1         IN     A       10.0.1.2
dns2         IN     A       10.0.1.3

ftp          IN     CNAME   server1
mail         IN     CNAME   server1
mail2        IN     CNAME   server2
www          IN     CNAME   server2
```

In diesem Beispiel werden Standard-Anweisungen und `SOA`-Werte verwendet. Die maßgeblichen Name-Server sind dabei als `dns1.example.com` und `dns2.example.com` eingestellt, die über `A`-Records verfügen, wodurch sie mit `10.0.1.2` bzw. `10.0.1.3` verbunden sind.

Die mit `MX`-Records konfigurierten E-Mail-Server verweisen auf `server1` und `server2` über `CNAME`-Records. Da die `server1`- und `server2`-Namen nicht mit einem Punkt enden (`.`), wird die `$ORIGIN`-Domain nach ihnen abgelegt, wobei sie zu `server1.domain.com` und `server2.domain.com` erweitert werden. Mit den dazugehörigen `A`-Resource-Records können dann ihre IP-Adressen bestimmt werden.

Die beliebten FTP- und Web-Dienste, die unter den standardmäßigen Namen `ftp.domain.com` und `www.domain.com` zur Verfügung stehen, verweisen auf Rechner, die entsprechende Dienste für die Namen bieten, die `CNAME`-Records verwenden.

11.3.4. Zone-Dateien für die umgekehrte Auflösung von Namen

Eine Zone-Datei für die Auflösung von Reverse-Namen wird verwendet, um eine IP-Adresse in ein bestimmtes Namespace in einem FQDN umzusetzen. Sie ähnelt einer standardmäßigen Zone-Datei, mit dem Unterschied, dass die `PTR`-Resource-Records zur Verknüpfung der IP-Adressen mit gültigen Domain-Namen verwendet werden.

Ein `PTR`-Record sieht Folgendem ähnlich:

```
<last-IP-digit>      IN     PTR    <FQDN-of-system>
```

Die *<last-IP-digit>* bezieht sich auf die letzte Nummer in einer IP-Adresse, mit der auf die FQDN eines bestimmtenSystems hingewiesen wird.

Im folgenden Beispiel werden die IP-Adressen `10.0.1.20` durch `10.0.1.25` den korrespondierenden FQDN zugewiesen.

```
$ORIGIN 1.0.10.in-addr.arpa
$TTL 86400
@      IN     SOA    dns1.example.com.     hostmaster.example.com. (
                     2001062501 ; serial
                     21600      ; refresh after 6 hours
                     3600       ; retry after 1 hour
                     604800     ; expire after 1 week
```

```
                        86400 )    ; minimum TTL of 1 day

      IN      NS      dns1.example.com.
      IN      NS      dns2.example.com.

20    IN      PTR     alice.example.com.
21    IN      PTR     betty.example.com.
22    IN      PTR     charlie.example.com.
23    IN      PTR     doug.example.com.
24    IN      PTR     ernest.example.com.
25    IN      PTR     fanny.example.com.
```

Diese Zone-Datei würde mit einer `zone`-Anweisung in der `named.conf`-Datei in den Dienst übernommen, was dann so ähnlich aussieht wie:

```
zone "1.0.10.in-addr.arpa" IN {
  type master;
  file "example.com.rr.zone";
  allow-update { none; };
};
```

Es gibt nur einen kleinen Unterschied zwischen diesem Beispiel und einer standardmäßigen `zone`-Direktive: der Name wird anders angegeben. Bitte beachten Sie, dass bei einer Zone für eine umgekehrte Auflösung die ersten drei Blöcke der IP-Adresse zum Umkehren benötigt werden und `.in-addr.arpa` danach angegeben ist. Dadurch kann ein einzelner Block von IP-Ziffern, der in der Zone-Datei zum umgekehrten Auflösen von Namen verwendet wird, richtig an diese Zone angefügt werden.

11.4. Die Verwendung von `rndc`

BIND enthält das Utility `rndc`, mit dem Sie den `named`-Daemon über die Befehlszeile vom lokalen und von einem Remote Host verwalten können.

Um zu verhindern, dass nicht authorisierte Benutzer Zugriff zum `named`-Daemon erlangen, verwendet BIND eine Authentifizierungsmethode, auf einem gemeinsamen geheimen Schlüssel basierend, um Hostsystemen den Zugriff zu gewähren. Das heisst, das ein übereinstimmender Schlüssel in `/etc/named.conf` und der `rndc` Konfigurationsdatei `/etc/rndc.conf` existieren muss.

11.4.1. Configuring `/etc/named.conf`

Um die Verbindung von `rndc`zu Ihrem `named`-Dienst zu ermöglichen, muss beim Start von `named` die `controls`-Anweisung in Ihrer `/etc/named.conf`-Datei vorhanden sein.

Das folgende Beispiel einer `controls`-Anweisung ermöglicht es Ihnen, `rndc`-Befehle vom lokalen Host auszuführen.

```
controls {
  inet 127.0.0.1 allow { localhost; } keys { <key-name>; };
};
```

Diese Anweisung weist `named` an, am standardmäßigen TCP-Port 953 nach Loopback-Adressen zu suchen und lässt `rndc`-Befehle zu, die vom lokalen Host ausgeführt werden, wenn der richtige Schlüssel angegeben wird. Der *<key-name>* bezieht sich auf die `key`-Direktive, die sich auch in der `/etc/named.conf`-Datei befindet. Im nächsten Beispiel wird eine `key`-Anweisung veranschaulicht.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
```

```
};
```

In diesem Beispiel benutzt <*key-value*> einen HMAC-MD5-Algorithmus. Mit dem nachfolgenden Befehl können Sie Ihre eigenen Schlüssel unter Verwendung eines HMAC-MD5-Algorithmus erstellen:

```
dnssec-keygen -a hmac-md5 -b <bit-length> -n HOST <key-file-name>
```

Es empfiehlt sich, einen Schlüssel mit einer Größe von mindestens 256 Bit zu erstellen. Der Schlüssel, der im <*key-value*>-Bereich gespeichert werden sollte, kann in der Datei <*key-file-name*>, welche von diesem Befehl erzeugt wurde, gefunden werden.

Warnung

Da `/etc/named.conf` von jedem gelesen werden kann, ist es angeraten, die `key`-Anweisung in eine separate Datei auszulagern, welche nur von root gelesen werden kann, und eine `include`-Anweisung zu verwenden, um diese Datei einzubinden, wie im folgenden Beispiel:

```
include "/etc/rndc.key";
```

11.4.2. Konfigurieren von `/etc/rndc.conf`

Die `key`-Anweisung ist die wichtigste in der Datei `/etc/rndc.conf`.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

<*key-name*> und <*key-value*> sollten exakt mit den Einstellungen in `/etc/named.conf` übereinstimmen.

Um den Schlüsseln, welche in `/etc/named.conf` auf dem Ziel-Server angegeben sind, zu entsprechen, fügen Sie folgende Zeilen zu `/etc/rndc.conf` hinzu.

```
options {
  default-server  localhost;
  default-key     "<key-name>";
};
```

Diese Anweisung setzt den globalen Default-Schlüssel. Die`rndc` Konfigurationsdatei kann allerdings auch verschiedene Schlüssel für verschiedene Server verwenden, wie im folgenden Beispiel gezeigt:

```
server localhost {
  key  "<key-name>";
};
```

Achtung

Stellen Sie sicher, dass jeweils nur ein root-Benutzer auf die Datei `/etc/rndc.conf` zugreifen kann.

Für weitere Informationen zur Datei `/etc/rndc.conf`, sehen Sie die `rndc.conf` man-Seiten.

11.4.3. Befehlszeilenoptionen

Ein `rndc`-Befehl sieht wie folgt aus:

`rndc <options> <command> <command-options>`

Wenn `rndc` auf einem korrekt konfigurierten lokalen Host ausgeführt wird, stehen Ihnen folgende Befehle zur Verfügung:

- `halt` — Hält den `named`-Service sofort an.
- `querylog` — Protokolliert alle Abfragen, die von Clients auf diesem Name-Server durchgeführt wurden.
- `refresh` — Aktualisiert die Datenbank des Nameservers.
- `reload` — Weist den Name-Server an, die Zone-Dateien neu zu laden, aber alle vorher verarbeiteten Antworten zu behalten. Dadurch können Sie Änderungen in den Zone-Dateien durchführen, ohne dass die gespeicherten Auflösungen von Namen verloren gehen.

  Wenn sich Ihre Änderungen nur auf eine bestimmte Zone auswirken, können Sie lediglich diese Zone neu laden. Geben Sie hierzu nach dem `reload`-Befehl den Namen der Zone ein.
- `stats` — Schreibt die aktuellen `named`-Statistiken in die Datei `/var/named/named.stats`.
- `stop` — Stoppt den Server vorsichtig, und speichert dabei alle dynamischen Updates und die vorhandenen *Incremental Zone Transfers* (*IXFR*) Daten, vor dem Beenden.

Gelegentlich werden Sie bestimmt auch die Standardeinstellungen in der `/etc/rndc.conf`-Datei übergehen wollen. Hierzu stehen Ihnen folgende Optionen zur Verfügung:

- `-c <configuration-file>` — Gibt einen alternativen Speicherort der Konfigurationsdatei an.
- `-p <port-number>` — Legt für die `rndc`-Verbindung eine andere als die standardmäßige Portnummer 953 fest.
- `-s <server>` — Ermöglicht es Ihnen, einen anderen als den `default-server` in `/etc/rndc.conf` anzugeben.
- `-y <key-name>` — Ermöglicht es Ihnen, einen anderen als den `default-key` in der `/etc/rndc.conf`-Datei einzustellen.

Zusätzliche Informationen zu diesen Optionen finden Sie auf der `rndc`-man-Seite

11.5. Erweiterte Funktionen von BIND

Die meisten BIND-Implementierungen verwenden für die Dienste zur Auflösung von Namen oder als Autorität für bestimmte Domains oder Sub-Domains nur `named`. Die Version 9 von BIND verfügt jedoch auch über eine Reihe weiterer Features, die - korrekte Konfigurierung und Verwendung vorausgesetzt - einen sichereren und effizienteren DNS-Dienst gewährleisten.

Achtung

Einige dieser Features, wie z.B. DNSSEC, TSIG und IXFR, sollten nur in Netzwerkumgebungen mit Nameservern verwendet werden, die diese Features unterstützen. Wenn Ihre Netzwerkumgebung nicht-BIND- oder ältere BIND-Nameserver enthält, prüfen Sie bitte, ob es dafür verbesserte Features gibt, bevor Sie sie verwenden.

Alle hier vorgestellten Features werden im *BIND 9 Administrator Reference Manual* detaillierter beschrieben. Unter Abschnitt 11.7.1 finden Sie mehr Informationen.

11.5.1. DNS-Protokoll-Erweiterungen

BIND unterstützt Incremental Zone Transfers (IXFR), bei denen Slave-Server nur die aktualisierten Teile einer Zone, die auf einem Master-Name-Server modifiziert wurden, heruntergeladen werden. Der standardmäßige TransferProcess erfordert, dass auch bei der kleinsten Änderung die gesamte Zone an alle Slave-Name-Server übermittelt wird. Für sehr populäre Domains mit sehr großzügigen Zone-Dateien und vielen Slave-Name-Servern macht IXFR den Benachrichtigungs- und Update-Prozess weniger ressourcenintensiv.

Beachten Sie bitte, dass IXFR nur zur Verfügung steht, wenn Sie für Änderungen der Master-Zonen-Records *dynamisch updaten*. Wenn Sie Zone-Dateien manuell bearbeiten, um Änderungen durchzuführen, verwenden Sie AXFR. Weitere Informationen über das dynamische Updaten finden Sie im *BIND 9 Administrator Reference Manual*. Unter Abschnitt 11.7.1 finden Sie mehr Informationen.

11.5.2. Mehrere Ansichten

Durch Verwendung der `view`-Anweisung in `named.conf`, kann BIND verschiedene Informationen bereitstellen, abhängig von welchem Netzwerk eine Anforderung gestellt wurde.

Dies ist vor allem dann nützlich, wenn Sie nicht möchten, dass externe Clients einen bestimmten DNS-Dienst ausführen oder bestimmte Informationen sehen können, während Sie dies auf dem lokalen Netzwerk internen Clients ermöglichen.

Die `view`-Anweisung verwendet die `match-clients`-Option, um IP-Adressen oder ganze Netzwerke zu vergleichen und diesen spezielle Optionen und Zone-Daten zu geben.

11.5.3. Sicherheit

BIND unterstützt eine Reihe verschiedener Methoden, um das Updaten von Zonen auf Master- oder Slave-Nameservern zu schützen:

- *DNSSEC* — Abkürzung für *DNS SECurity*. Dieses Feature ist für Zonen, die mit einem *Zonenschlüssel* kryptographisch signiert werden, bestimmt.

  Auf diese Weise kann sichergestellt werden, dass die Informationen über eine spezielle Zone von einem Nameserver stammen, der mit einem bestimmten privaten Schlüssel signiert wurde, und der Empfänger über den öffentlichen Schlüssel dieses Nameservers verfügt.

  Version 9 von BIND unterstützt auch die SIG(0) öffentlicher/privater Schlüssel Methode für die Authentifizierung von Nachrichten.

- *TSIG* — Abkürzung für *Transaction SIGnatures*. Dieses Feature erlaubt die Übertragung von Master zu Slave nur dann, wenn ein gemeinsam verwendeter geheimer Schlüssel auf beiden Name-Servern existiert.

Dieses Feature unterstützt die auf der IP-Adresse basierende Methode der Transfer-Authorisierung. Somit muss ein unerwünschter Benutzer nicht nur Zugriff auf die IP-Adresse haben, um die Zone zu übertragen, sondern auch den geheimen Schlüssel kennen.

Version 9 von BIND unterstützt auch *TKEY*, eine weitere Methode der Autorisierung von Zone-Übertragungen auf der Basis eines gemeinsam verwendeten geheimen Schlüssels.

11.5.4. IP-Version 6

Die Version 9 von BIND kann mit den `A6` Zone-Records Name-Service für die IP-Version 6 (IPv6)-Umgebungen zur Verfügung stellen.

Wenn Ihre Netzwerkumgebung sowohl über Ipv4- als auch IPv6-Hosts verfügt, können Sie den `lwresd` Lightweight Resolver Daemon in Ihren Netzwerk-Clients verwenden. Dieser Daemon ist ein sehr effektiver Caching-Only-Name-Server, der die neuesten `A6`- und `DNAME`-Records versteht, die mit Ipv6 verwendet werden. Auf der `lwresd`-man-Seite finden Sie weitere Informationen hierzu.

11.6. Allgemein zu vermeidende Fehler

Es kommt häufig vor, dass Anfänger bei der Bearbeitung der Konfigurationsdateien von BIND Fehler machen oder bei der Verwendung von `named` zunächst Schwierigkeiten haben. Viele der nachfolgend beschriebenen Probleme können Sie aber vermeiden, wenn Sie Folgendes beachten:

- *Erhöhen Sie die Seriennummer, wenn Sie eine Zone-Datei bearbeiten.*

  Wenn die Seriennummer nicht erhöht wird, hat Ihr Master-Name-Server zwar die korrekten neuen Informationen, Ihr Slave-Name-Server werden jedoch nie über diese Änderungen oder den Versuch informiert, die Daten in der Zone zu aktualisieren.

- *Achten Sie darauf, dass Sie geschweifte Klammern und Strichpunkte in der `/etc/named.conf`-Datei richtig verwenden.*

  Ein ausgelassenes Semikolon oder eine nicht geschlossene geschweifte Klammer kann dazu führen, dass `named` nicht startet.

- *Denken Sie daran, in den Zone-Dateien nach jedem FQDN Punkte (`.`) zu setzen und sie beim Hostnamen wegzulassen.*

  Der Punkt bedeutet, dass der angegebene Name komplett ist. Wird er weggelassen, platziert `named` den Namen der Zone oder des `$ORIGIN`-Werts hinter den Namen, um ihn zu vervollständigen.

- *Wenn Ihre Firewall Verbindungen von Ihrem `named` zu anderen Nameservern blockiert, müssen Sie möglicherweise die Konfigurationsdatei bearbeiten.*

  Standardmäßig verwendet die Version 9 von BIND willkürliche Ports oberhalb von 1024, um andere Name-Server abzufragen. Einige Firewalls gehen jedoch von Name-Servern aus, die für die Kommunikation nur den Port 53 verwenden. Sie können dieses Verhalten erzwingen, indem Sie in `/etc/named.conf` folgende Zeile zur `options`-Direktive hinzufügen:

  ```
  query-source address * port 53;
  ```

11.7. Zusätzliche Ressourcen

Folgende Quellen enthalten zusätzliche Hintergrundinformationen zu BIND.

11.7.1. Installierte Dokumentation

- BIND verfügt über installierte Dokumentationen, die verschiedene Themen behandeln und jeweils in einem eigenen Verzeichnis abgelegt sind:
  - `/usr/share/doc/bind-<version-number>/` — Eine Auflistung der neuesten Features, wobei <version-number> die auf Ihrem System installierte Version von `bind` ist.
  - `/usr/share/doc/bind-<version-number>/arm/` — Enthält das *BIND 9 Administrator Reference Manual* im HTML- und SGML-Format, mit Details über die für BIND erforderlichen Ressourcen, zur Konfigurationsweise der verschiedenen Name-Server-Typen, zur Durchführung des Load-Balancing und anderen spezielleren Themen. Die meisten neuen Benutzer werden sich mit dieser Informationsquelle am besten mit BIND vertraut machen können. <version-number> ist dabei die auf Ihrem System installierte Version von `bind`.
  - `/usr/share/doc/bind-<version-number>/draft/` — Enthält ausgewählte technische Dokumente, die sich mit dem DNS Service und damit verbundenen Problemen beschäftigen und einige Methoden zur Lösung dieser Probleme vorschlagen. <version-number> ist dabei die auf Ihrem System installierte Version von `bind`.
  - `/usr/share/doc/bind-<version-number>/misc/` — Enthält Dokumente über spezielle verbesserte Merkmale. Benutzer der Version 8 von BIND sollten sich das Dokument `migration` anschauen, das sich mit bestimmten Änderungen befasst, die für eine Verwendung der Version 9 von BIND vorzunehmen sind. In der `options`-Datei sind alle in BIND 9 implementierten Optionen aufgelistet, die in `/etc/named.conf` verwendet werden. <version-number> ist dabei die auf Ihrem System installierte Version von `bind`.
  - `/usr/share/doc/bind-<version-number>/rfc/` — In diesem Verzeichnis finden Sie jedes RFC-Dokument, das mit BIND zusammenhängt. <version-number> ist dabei die auf Ihrem System installierte Version von `bind`.

- BIND-bezogene man-Seiten — Es gibt einige man-Seiten zu den verschiedenen Applikationen und Konfigurationsdateien die im Bezug zu BIND stehen. Einige der wichtigeren sind Folgend aufgelistet.

  Administrative Applikationen

  - `man rndc` — Erklärt die verschiedenen Optionen, die bei der Verwendung von `rndc` zur Kontrolle eines BIND Name-Servers zur Verfügung stehen.

  Server-Applikationen

  - `man named` — Untersucht ausgewählte Argumente, die zur Steuerung des BIND-Name-Server-Daemon verwendet werden können.
  - `man lwresd` — Beschreibt den Lightweight-Resolver-Daemon und dessen verfügbare Optionen.

  Konfigurationsdateien

  - `man named.conf` — Eine vollständige Liste von Optionen, welche in der `named`-Konfigurationsdatei zur Verfügung stehen.

- `man rndc.conf` — A Eine vollständige Liste von Optionen, welche in der `rndc`-Konfigurationsdatei zur Verfügung stehen.

11.7.2. Hilfreiche Webseiten

- http://www.isc.org/products/BIND/ — Die Homepage des BIND-Projekts. Hier finden Sie Informationen aktuellen Releases und können das *BIND 9 Administrator Reference Manual* in der PDF-Version herunterladen.
- http://www.redhat.com/mirrors/LDP/HOWTO/DNS-HOWTO.html — Befasst sich mit BIND als Caching-Nameserver und der Konfiguration der einzelnen Zone-Dateien sowie der Konfiguration verschiedener Zone-Dateien, die als primärer Name-Server für eine Domain benötigt werden.

11.7.3. Bücher zum Thema

- *Red Hat Enterprise Linux Handbuch zur System-Administration* — Das Kapitel *BIND-Konfiguration* erklärt wie man mit Hilfe des**Domain Name Service Configuration Tool** einen DNS-Server einrichten kann.
- *DNS and BIND* von Paul Albitz und Cricket Liu; O'Reilly & Associates — Ein bekanntes Buch, das allgemeine und weiterführende Optionen der Konfiguration von BIND erklärt und Strategien zum Schutz Ihres DNS-Servers vorstellt.
- *The Concise Guide to DNS and BIND* von Nicolai Langfeldt; Que — Beschreibt die Verbindungen zwischen mehreren Netzwerkdiensten und BIND mit Schwerpunkt auf aufgabenorientierten technischen Themen.

Kapitel 12.

Lightweight Directory Access Protocol (LDAP)

LDAP (*Lightweight Directory Access Protocol*) ist ein Satz von offenen Protokollen, die zum Zugreifen auf zentral gespeicherte Informationen über ein Netzwerk verwendet werden. Es basiert auf dem *X.500*-Standard für das gemeinsame Nutzen von Verzeichnissen, ist jedoch weniger komplex und ressourcenintensiv. Aus diesem Grund wird LDAP bisweilen auch *X.500 Lite* genannt.

Ebenso wie X.500 organisiert LDAP die Informationen mit Hilfe von Verzeichnissen hierarchisch. In den Verzeichnissen kann eine Vielfalt an Informationen gespeichert werden. Zudem können sie auf ähnliche Weise wie der Network Information Service (NIS) verwendet werden, so dass alle Benutzer von jedem beliebigen Rechner in einem LDAP-unterstützten Netzwerk auf ihre Accounts zugreifen können.

In den meisten Fällen wird LDAP jedoch einfach als virtuelles Telefonbuch verwendet, mit dem Benutzer auf Kontaktinformationen für andere Benutzer zugreifen können. LDAP geht allerdings über ein herkömmliches Telefonbuch hinaus, da es seine Verzeichnisse auf andere LDAP-Server weltweit übertragen und somit globalen Zugriff auf Informationen zur Verfügung stellen kann. Momentan wird LDAP allerdings in der Regel eher in Einzelorganisationen wie Universitäten, Regierungsabteilungen und Privatunternehmen verwendet.

LDAP ist ein Client-/Server-System. Der Server kann eine Vielfalt an Datenbanken zum Speichern eines Verzeichnisses verwenden, wobei jede für schnelle und umfangreiche Lesevorgänge optimiert ist. Wenn eine LDAP-Clientanwendung eine Verbindung mit einem LDAP-Server herstellt, kann sie entweder ein Verzeichnis abfragen oder Informationen hochladen. Im Fall einer Abfrage antwortet der Server entweder auf die Abfrage oder, wenn er nicht lokal antworten kann, verweist er den Anfrage-Upstream an einen übergeordneten LDAP-Server weiter, der die Antwort übernimmt. Versucht die Clientanwendung, Informationen in ein LDAP-Verzeichnis zu laden, prüft der Server, ob der Benutzer zum Ausführen der Änderung berechtigt ist und fügt dann die Informationen hinzu bzw. aktualisiert sie.

In diesem Kapitel wird die Konfiguration und Verwendung von OpenLDAP 2.0, einer Open-Source-Implementierung der LDAPv2- und LDAPv3-Protokolle behandelt.

12.1. Warum LDAP?

Der Hauptvorteil von LDAP ist die Verdichtung von bestimmten Informationen für eine gesamte Organisation in ein zentrales Repository. So kann LDAP zum Beispiel für das Verwalten von Benutzerlisten für alle Gruppen einer Organisation als ein zentrales Verzeichnis verwendet werden, auf das vom gesamten Netzwerk aus zugegriffen werden kann. Und da LDAP SSL (Secure Sockets Layer) und TLS (Transport Layer Security) unterstützt, können sensible Daten vor neugierigen Augen geschützt werden.

LDAP unterstützt auch viele Backend-Datenbanken, in denen die Verzeichnisse gespeichert werden. Die Administratoren verfügen hierdurch über die notwendige Flexibilität, eine Datenbank bereitzustellen, die für die Informationsarten, die der Server verbreiten soll, optimal angepasst ist. Des Weiteren verfügt LDAP über eine gut durchdachte API (Application Programming Interface), und es sind auch zahlreiche LDAP-fähige Applikationen vorhanden, deren Anzahl und Qualität zunimmt.

12.1.1. Funktionserweiterungen von OpenLDAP 2.0

OpenLDAP 2.0 umfasst zahlreiche wichtige Funktionen.

- *LDAPv3 Support* — OpenLDAP 2.0 unterstützt SASL (Simple Authentication and Security Layer), TLS (Transport Layer Security) und SSL (Secure Sockets Layer) neben weiteren Verbesserungen.

Viele Änderungen, die seit LDAPv2 am Protokoll vorgenommen wurden, sollen zur Sicherheit von LDAP beitragen.

- *IPv6 Support* — OpenLDAP unterstützt die nächste Generation des Internetprotokolls, Version 6.
- *LDAP Over IPC* — OpenLDAP kann innerhalb eines bestimmten Systems mit Hilfe von IPC (Interprocess Communication) kommunizieren. Das Umgehen der Kommunikation über ein Netzwerk erhöht die Sicherheit.
- *Aktualisierte C API* — Verbessert die Art und Weise, in welcher Programmierer zu LDAP Verzeichnis-Servern verbinden und mit diesen arbeiten.
- *LDIFv1 Support* — OpenLDAP 2.0 ist mit LDAP Data Interchange Format (LDIF) Version 1 voll kompatibel.
- *Verbesserter Stand-Alone LDAP Server* — OpenLDAP enthält jetzt ein aktualisiertes Zugriffssteuerungssystem, Thread-Pooling, bessere Tools und vieles mehr.

12.2. LDAP Terminologie

Jede Diskussion des LDAP erfordert ein grundlegendes Verständnis einiger LDAP-spezifischen Begriffe:

- *Eintrag* — Ein Eintrag (Entry) stellt in einem LDAP-Verzeichnis eine Einheit dar. Ein Eintrag wird durch seinen eindeutigen Namen (*Distinguished Name, kurz DN*) identifiziert.
- *Attribute* — Attribute sind direkt mit dem Eintrag zusammenhängende Informationen. Eine Organisation könnte zum Beispiel ein LDAP-Eintrag sein. Mit dieser Organisation verknüpfte Attribute können zum Beispiel die Faxnummer, die Adresse usw. sein. Auch Mitarbeiter können Einträge in einem LDAP-Verzeichnis sein. Übliche Attribute für Mitarbeiter sind u.a. Telefonnummern und E-Mail-Adressen.

  Bestimmte Attribute sind obligatorisch, während andere Attribute optional sind. In einer *Objektklasse* (Objectclass) ist festgelegt, welche Attribute pro Eintrag obligatorisch und welche optional sind. Die Objektklassendefinitionen sind in verschiedenen Schemadateien im Verzeichnis `/etc/openldap/schema` abgelegt. Für mehr Information zu LDAP Schemata, siehe Abschnitt 12.5.
- *LDIF* — Das *LDAP-Datenaustauschformat* (LDAP Data Interchange Format, LDIF) ist ein ASCII-Textformat für LDAP-Einträge. Dateien, die Daten von einem LDAP-Server importieren oder auf einen LDAP-Server exportieren, müssen im LDIF-Format vorliegen. Ein LDIF-Eintrag sieht zum Beispiel folgendermaßen aus:

  ```
  [<id>]
  dn: <distinguished name>
  <attrtype>: <attrvalue>
  <attrtype>: <attrvalue>
  <attrtype>: <attrvalue>
  ```

  Ein Eintrag kann so viele der `<attrtype>: <attrvalue>` Paare haben, wie erforderlich. Eine leere Zeile markiert das Ende eines Eintrags.

Achtung

Alle der `<attrtype>` und `<attrvalue>` Paare *müssen* in einer entsprechenden Schemadatei definiert sein, um diese Informationen verwenden zu können.

Alle Angaben innerhalb der spitzen Klammern "<" und ">" sind Variablen und können mit Ausnahme von `<ID>` beim Erstellen eines neuen LDAP-Eintrags festgelegt werden. Die `<ID>` ist eine Zahl, die von der Anwendung festgelegt wird, wenn der Eintrag bearbeitet wird.

12.3. OpenLDAP Daemons and Utilities

Die Suite der OpenLDAP Bibliotheken und Tools ist über folgende Pakete verteilt:

- `openldap` — Enthält die Bibliotheken welche zum Ausführen der OpenLDAP Server- und Client-Applikationen benötigt werden.
- `openldap-clients` — Enthält die Befehlszeilentools zur Ansicht und zum Verändern der Verzeichnisse auf einem LDAP-Server.
- `openldap-server` — Enthält die Server und andere Tools, welche zum Konfigurieren und für den Betrieb eines LDAP Servers benötigt werden.

Das `openldap-servers`-Paket enthält zwei Server: den *Standalone LDAP Daemon* (`/usr/sbin/slapd`) und den *Standalone LDAP Update Replication Daemon* (`/usr/sbin/slurpd`).

Der `slapd`-Daemon ist der eigenständige LDAP-Server, während der `slurpd`-Daemon zum Synchronisieren der Änderungen von einem LDAP-Server auf andere LDAP-Server im Netzwerk verwendet wird. Der `slurpd`-Daemon ist nur erforderlich, wenn mehrere LDAP-Server verwendet werden.

Das `openldap-server`-Paket installiert zum Durchführen von Verwaltungsaufgaben folgende Utilities in `/usr/sbin`:

- `slapadd` — Fügt Einträge aus einer LDIF-Datei in ein LDAP-Verzeichnis ein. `/usr/sbin/slapadd -l` *`ldif-Eingabe`* liest die LDIF-Datei, *`ldif-Eingabe`*, welche die neuen Einträge enthält.
- `slapcat` — Entnimmt Einträge aus einem LDAP-Verzeichnis im Standardformat — Berkeley DB — und speichert diese in einer LDIF-Datei. Der Befehl `/usr/sbin/slapcat -l` *`ldif-Ausgabe`* gibt zum Beispiel eine LDIF-Datei *`ldif-Ausgabe`* aus, welche die Einträge aus dem LDAP-Verzeichnis enthält.
- `slapcat-gdbm` — Zieht Einträge aus dem LDAP-Verzeichnis im gdbm-Format (die Vorgabe in früheren OpenLDAP-Versionen) und speichert diese in einer LDIF-Datei. Dieser Befehl wird lediglich zur Migration eines Verzeichnisses von OpenLDAP unter Red Hat Enterprise Linux 2.1 und Red Hat Linux Versionen 7.x bis 8 verwendet. Sehen Sie Abschnitt 12.8 für Informationen zur Verwendung dieses Befehls.
- `slapindex` — Indiziert das `slapd`-Verzeichnis auf Grundlage des aktuellen Inhalts neu. Dieses Tools sollte ausgeführt werden, wenn die Indexing-Optionen in `/etc/openldap/slapd.conf` geändert werden.
- `slappasswd` — Generiert einen verschlüsselten Wert eines Benutzerpasswortes zur Verwendung mit dem `ldapmodify`- oder `rootpw`-Wert in der slapd-Konfigurationsdatei `/etc/openldap/slapd.conf`. Führen Sie `/usr/sbin/slappasswd` aus, um das Passwort zu erstellen.

Warnung

Stellen Sie sicher, dass `slapd` mit Hilfe von `/usr/sbin/service slapd stop` angehalten wird, bevor Sie `slapadd`, `slapcat` oder `slapindex` verwenden. Andernfalls riskieren Sie die Integrität des LDAP-Verzeichnis.

Weitere Informationen zur Verwendung dieser Utilities finden Sie auf den jeweiligen man-Seiten.

Das `openldap-clients`-Paket installiert Tools zum Hinzufügen, Ändern und Löschen von Einträgen eines LDAP-Verzeichnisses in `/usr/bin/`. Diese Tools beinhalten Folgendes:

- `ldapmodify` — Ändert Einträge in einem LDAP-Verzeichnis durch Eingaben aus einer Datei oder von der Standardeingabe.
- `ldapadd` — Fügt durch Annehmen von Eingaben über eine Datei oder der Standardeingabe Einträge zum Verzeichnis hinzu. `ldapadd` ist nichts anderes als ein harter Link zu `ldapmodify -a`.
- `ldapdelete` — Löscht Einträge aus einem LDAP-Verzeichnis durch Annehmen von Eingaben des Benutzers am Terminal oder über eine Datei.
- `ldapmodify` — Ändert Einträge in einem LDAP-Verzeichnis durch Eingaben aus einer Datei oder von der Standardeingabe.
- `ldappasswd` — Setzt das Passwort für einen LDAP-Benutzer.
- `ldapsearch` — Sucht mit Hilfe eines Shell-Prompts im LDAP-Verzeichnis nach Einträgen.

Alle Utilities, `ldapsearch` ausgenommen, sind einfacher durch Verweisen auf eine Datei mit den vorzunehmenden Änderungen zu verwenden, als durch Eingabe eines Befehls für jeden Eintrag, der in einem LDAP-Verzeichnis geändert werden soll. Das Format solcher Dateien wird auf der man-Seite der jeweiligen Applikation skizziert.

12.3.1. NSS, PAM, and LDAP

Neben den OpenLDAP-Paketen enthält Red Hat Enterprise Linux das Paket `nss_ldap`, das die Möglichkeit LDAP in Linux- und andere UNIX-Umgebungen zu integrieren optimiert.

Das Paket `nss_ldap` stellt folgende Module zur Verfügung:

- `/lib/libnss_ldap-<glibc-version>.so`
- `/lib/security/pam_ldap.so`

Die `libnss_ldap-<glibc-version>.so` Module ermöglichen Applikationen, Benutzer, Gruppen, Hosts und sonstige Informationen mit Hilfe eines LDAP-Verzeichnisses über die Schnittstelle *Nameservice Switch* (NSS) zu suchen (ersetzen Sie `<glibc-version>` mit der verwendeten Version von `libnss_ldap`). NSS erlaubt Applikationen eine Authetifizierung unter Verwendung von LDAP in Verbindung mit dem Name-Service *Network Information Service* (NIS) und Klartext-Authentifizierungsdateien.

Das Modul `pam_ldap` ermöglicht PAM-fähigen Applikationen, Benutzer mit Hilfe von in einem LDAP-Verzeichnis gespeicherten Informationen zu authentifizieren. PAM-fähige Applikationen umfassen Konsolenanmeldung, POP- und IMAP-Mail-Server und Samba. Wenn ein LDAP-Server im Netzwerk bereitgestellt wird, können alle Anmeldesituationen gegen eine Benutzer-ID und Passwortkombination authentifizieren und so die Verwaltung spürbar vereinfachen.

12.3.2. PHP4, LDAP und Apache HTTP Server

Red Hat Enterprise Linux enthält auch Pakete mit LDAP-Modulen für die PHP-serverseitige Skriptsprache.

Das Paket `php-ldap` fügt LDAP-Unterstützung zur PHP4 HTML-eingebetteten Skriptsprache über das Modul `/usr/lib/php4/ldap.so` hinzu. Dieses Modul ermöglicht PHP4-Skripten, auf Informationen zuzugreifen, die in einem LDAP-Verzeichnis gespeichert sind.

Red Hat Enterprise Linux wird mit dem Modul `mod_authz_ldap` für Apache HTTP Server ausgeliefert. Dieses Modul verwendet die Kurzform des "Distinguished Name" als Subjekt und den Aussteller des Client-SSL-Zertifikats, um den "Distinguished Name" des Benutzers innerhalb eines LDAP-Verzeichnisses zu bestimmen. Es kann auch Benutzer anhand den Attributen der Einträge im LDAP-Verzeichnis autorisieren, wobei Zugriff auf ein Asset auf Benutzerrechte und Gruppenrechten des Asset basiert und Zugriff für Benutzer mit abgelaufenen Passwörtern abgelehnt wird. Das Modul `mod_ssl` wird für die Verwendung des Modul `mod_authz_ldap` benötigt.

Wichtig

Das Modul `mod_authz_ldap` authetifiziert einen Benutzer zu einem LDAP-Verzecihnis mit einem verschlüsselten Passwort-Hash. Diese Funktionalität ist im experimentellen Modul `mod_auth_ldap` enthalten, das nicht in Red Hat Enterprise Linux enthalten ist. Sehen Sie die Website der Apache Software Foundation Online unter http://www.apache.org/ für Informationen zum Status dieses Moduls.

12.3.3. LDAP Client-Applikationen

Es stehen grafische LDAP-Clients zur Verfügung, die das Erstellen und Ändern von Verzeichnissen unterstützen. Diese sind allerdings nicht im Lieferumfang von Red Hat Enterprise Linux enthalten. Eine solche Anwendung ist **LDAP Browser/Editor** — Ein Java-basiertes Tool, das unter http://www.iit.edu/~gawojar/ldap zur Verfügung steht.

Die meisten anderen LDAP-Clients greifen auf die Verzeichnisse im Lesemodus zu und verwenden sie zum Verweisen (und nicht Ändern) auf unternehmensweite Informationen. Beispiele für diese Anwendungen sind Sendmail, **Mozilla**, **Gnome Meeting**, und **Evolution**.

12.4. OpenLDAP Konfigurationsdateien

Die Konfigurationsdateien von OpenLDAP werden im Verzeichnis `/etc/openldap/` installiert. Im Folgenden werden die wichtigsten Verzeichnisse und Dateien kurz vorgestellt:

- `/etc/openldap/ldap.conf` — Dies ist die Konfigurationsdatei für alle *Client*-Applikationen, die die OpenLDAP-Bibliotheken verwenden. Darunter befinden sich unter anderem `ldapsearch`, `ldapadd`, Sendmail, **Evolution**, und **Gnome Meeting**.
- `/etc/openldap/slapd.conf` — Dies ist die Konfigurationsdatei für den `slapd`-Daemon. Weitere Informationen zu dieser Datei finden Sie unter Abschnitt 12.6.1.
- `/etc/openldap/schema/`-Verzeichnis — Dieses Unterverzeichnis enthält das vom `slapd`-Daemon verwendete Schema. Weitere Informationen zu diesem Verzeichnis finden Sie unter Abschnitt 12.5.

Anmerkung

Wenn das `nss_ldap`-Paket installiert ist, erstellt es die Datei `/etc/ldap.conf`. Diese Datei wird von den PAM- und NSS-Modulen verwendet, die vom `nss_ldap`-Paket bereitgestellt werden. Weitere Informationen zu dieser Konfigurationsdatei finden Sie unter Abschnitt 12.7.

12.5. Das Verzeichnis `/etc/openldap/schema/`

Das `/etc/openldap/schema/`-Verzeichnis beinhaltet die LDAP-Definition, die zuvor in den Dateien `slapd.at.conf` und `slapd.oc.conf` abgelegt waren. Alle *Attributsyntaxdefinitionen* und *Objektklassendefinitionen* sind jetzt in den unterschiedlichen Schemadateien abgelegt. Auf die verschiedenen Schemadateien wird in `/etc/openldap/slapd.conf` mit Hilfe der `include`-Zeilen verwiesen, wie im folgenden Beispiel zu sehen ist:

```
include  /etc/openldap/schema/core.schema
```

```
include  /etc/openldap/schema/cosine.schema
include  /etc/openldap/schema/inetorgperson.schema
include  /etc/openldap/schema/nis.schema
include  /etc/openldap/schema/rfc822-MailMember.schema
include  /etc/openldap/schema/autofs.schema
include  /etc/openldap/schema/kerberosobject.schema
```

Achtung

Sie sollten keines der Schemata aus den, von OpenLDAP installierten, Schemadateien ändern.

Sie können das von OpenLDAP verwendete Schema erweitern, um zusätzliche Attributtypen und Objektklassen mit Hilfe der Standardschemadateien zu unterstützen. Erstellen Sie dafür eine `local.schema`-Datei im Verzeichnis `/etc/openldap/schema`. Referenzieren Sie dieses neue Schema in `slapd.conf`, indem Sie die folgende Zeile unter die standardmäßigen `include`-Schemazeilen hinzufügen:

```
include          /etc/openldap/schema/local.schema
```

Definieren Sie anschließend Ihre neuen Attributtyen und Objektklassen der `local.schema`-Datei. Viele Organisationen verwenden die standardmäßig installierten Attributtypen und Objektklassen der Schemadateien und modifizieren diese für die Verwendung in der `local.schema`-Datei.

Das Erweitern der Schemata zum Erreichen spezieller Anforderungen ist reichlich komplex und übersteigt den Umfang dieses Kapitels. Weitere Informationen über die Erstellung neuer Schemadateien finden Sie unter http://www.openldap.org/doc/admin/schema.html.

12.6. Überblick über die OpenLDAP-Einrichtung

In diesem Abschnitt wird ein kurzer Überblick über das Installieren und Konfigurieren eines OpenLDAP-Verzeichnisses gegeben. Weitere Details finden Sie unter folgenden URLs:

- http://www.openldap.org/doc/admin/quickstart.html — Der *Quick-Start Guide* auf der OpenLDAP-Website.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — *LDAP Linux HOWTO* vom Linux Documentation Project, das auf der Website von Red Hat gespiegelt ist.

Die Grundschritte zum Erstellen eines LDAP-Servers sind folgende:

1. Installieren Sie die RPMs `openldap`, `openldap-servers` und `openldap-clients`.
2. Bearbeiten Sie die Datei `/etc/openldap/slapd.conf`, um auf die LDAP-Domain und den LDAP-Server zu verweisen. Weitere Informationen finden Sie unter Abschnitt 12.6.1.
3. Starten Sie `slapd` mit folgendem Befehl:
   `/sbin/service/ldap start`

   Nachdem Sie LDAP konfiguriert haben, können Sie `chkconfig`, `ntsysv` oder **Services Configuration Tool** verwenden, um LDAP so zu konfigurieren, dass es zur Bootzeit gestartet wird. Weitere Informationen zum Konfigurieren von Services finden Sie im Kapitel *Kontrolle des Zugriffs auf die Services* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.
4. Fügen Sie Einträge zum LDAP-Verzeichnis mit Hilfe von `ldapadd` hinzu.
5. Verwenden Sie `ldapsearch`, um zu prüfen, ob `slapd` auf die Informationen richtig zugreift.

6. Wenn Sie an diesem Punkt angelangt sind, sollte Ihr LDAP-Verzeichnis ordnungsgemäß funktionieren, und Sie können alle LDAP-fähigen Applikationen für die Verwendung des LDAP-Verzeichnisses konfigurieren.

12.6.1. Bearbeiten des Verzeichnisses `/etc/openldap/slapd.conf`

Sie müssen die Konfigurationsdatei `/etc/openldap/slapd.conf` des `slapd`-LDAP-Servers ändern, um ihn verwenden zu können. Sie müssen diese Datei bearbeiten, um sie an Ihre Domain und Server anzupassen.

Die `Suffix`-Zeile nennt die Domain, für die der LDAP-Server Informationen bereitstellt und sollte wie folgt geändert werden:

```
suffix          "dc=your-domain,dc=com"
```

Hier muss ein gültiger Domainname eingetragen werden. Zum Beispiel:

```
suffix          "dc=example,dc=com"
```

Der Eintrag `rootdn` ist der eindeutige Name (Distinguished Name, kurz DN) für einen Benutzer, der keinen Einschränkungen durch Parameter der Zugriffssteuerung oder Benutzerverwaltung unterliegt, die im LDAP-Verzeichnis für Vorgänge festgelegt sind. Der Benutzer `rootdn` ist sozusagen Root für das LDAP-Verzeichnis. Die `rootdn`-Zeile ist zu ändern in:

```
rootdn          "cn=root,dc=example,dc=com"
```

Wenn Sie vorhaben, dass LDAP-Verzeichnis übers Netzwerk zu verwalten, ändern Sie die `rootpw`-Zeile — indem Sie den Standardwert mit einem verschlüsselten Passwort ersetzen. Um ein verschlüsseltes Passwort zu erzeugen, geben Sie den folgenden Befehl ein:

```
slappasswd
```

Sie werden dazu aufgefordert, ein Passwort einzugeben, und durch eine zweite Eingabe zu bestätigen. Danach gibt das Programm das verschlüsselte Passwort am Terminal aus.

Als nächstes, kopieren Sie das neu erzeugte verschlüsselte Passwort in die Datei `/etc/openldap/slapd.conf` in eine der `rootpw`-Zeilen, und entfernen Sie das Hash-Symbol (`#`).

Nach Abschluss, sollte die `rootpw`-Zeile etwa wie folgt aussehen:

```
rootpw {SSHA}vv2y+i6V6esazrIv70xSSnNAJE18bb2u
```

Warnung

LDAP-Passwörter, einschließlich der in `/etc/openldap/slapd.conf` angegebenen `rootpw`-Direktive werden als Klartext über das Netzwerk gesendet, es sei denn, Sie aktivieren die TLS-Verschlüsselung.

Um TLS-Verschlüsselung zu aktivieren, sehen Sie die Kommentare in `/etc/openldap/slapd.conf` und die man-Seite für `slapd.conf`.

Für zusätzliche Sicherheit sollte die `rootpw`-Direktive auskommentiert werden, indem ihr ein Hash-Symbol (#) vorangestellt wird.

Wenn Sie das Befehlszeilentool `/usr/bin/slapadd` verwenden, um das LDAP-Verzeichnis lokal aufzufüllen, müssen Sie die `rootpw`-Direktive nicht verwenden.

Wichtig

Sie müssen root sein um `/usr/sbin/slapadd` verwenden zu können. Der Verzeichnis-Server wird jedoch als Benutzer `ldap` ausgeführt. Der Verzeichnis-Server ist deshalb nicht in der Lage, Dateien, welche von `slapadd` erzeugt wurden, zu ändern. Um dieses Problem zu beheben, geben Sie den folgenden Befehl ein, nachdem Sie `slapadd` beendet haben:

```
chown -R ldap /var/lib/ldap
```

12.7. Konfigurieren Ihres Systems für die Authentifizierung mit OpenLDAP

Dieser Abschnitt gibt einen kurzen Überblick über die Konfiguration der OpenLDAP Benutzer-Authentifizierung. Wenn Sie kein OpenLDAP-Experte sind, benötigen Sie wahrscheinlich eine umfassendere Dokumentation, als wir Ihnen hier bieten können. Weitere Informationen finden Sie in den in Abschnitt 12.9 angegebenen Literaturhinweisen.

Installieren der notwendigen LDAP-Pakete

Zuerst sollten Sie sicherstellen, dass die erforderlichen Pakete auf beiden, dem LDAP-Server und dem LDAP-Client installiert sind. Der LDAP-Server benötigt das `openldap-server` Paket.

Die Pakete `openldap`, `openldap-clients`, und `nss_ldap` müssen auf allen LDAP Client-Maschinen installiert sein.

Bearbeiten der Konfigurationsdateien

- Bearbeiten Sie die Datei `/etc/openldap/slapd.conf` auf dem LDAP-Server, um sicherzustellen, dass diese mit den Gegebenheiten Ihrer Organisation übereinstimmt. Bitte sehen Sie Abschnitt 12.6.1 für Anleitungen zum Bearbeiten der Datei `slapd.conf`.
- Auf allen Client-Rechnern müssen sowohl `/etc/ldap.conf` als auch `/etc/openldap/ldap.conf` den jeweiligen Server und grundlegende Informationen für Ihre Organisation enthalten.

  Die einfachste Weise hierzu ist das Ausführen von **Authentication Configuration Tool** (`authconfig-gtk`) und das Auswählen von **LDAP verwenden** in der Tab **Benutzerinformationen**.

  Diese Dateien können auch manuell bearbeitet werden.
- Auf allen Client-Maschinen, muss die Datei `/etc/nsswitch.conf` bearbeitet werden um LDAP zu verwenden.

  Die einfachste Weise hierzu ist das Ausführen von **Authentication Configuration Tool** (`authconfig-gtk`) und das Auswählen von **LDAP verwenden** in der Tab **Benutzerinformationen**.

  Wenn Sie `/etc/nsswitch.conf` manuell bearbeiten, fügen Sie `ldap` in den entsprechenden Zeilen hinzu.

  Zum Beispiel:

  ```
  passwd: files ldap
  shadow: files ldap
  group: files ldap
  ```

12.7.1. PAM and LDAP

Führen Sie `Authentication Configuration Tool` (`authconfig-gtk`) aus, und wählen Sie die Option **LDAP verwenden** im Tab **Authentifizierung** aus, damit Sie standardmäßige PAM-fähige Anwendungen für die Authentifizierung mit LDAP verwenden können. Weitere Informationen zum Konfigurieren von PAM finden Sie unter Kapitel 13 sowie auf den man-Seiten von PAM.

12.7.2. Umwandeln Ihrer alten Authentifizierungsinformationen in das LDAP-Format

Das Verzeichnis `/usr/share/openldap/migration/` enthält mehrere Shell- und Perl-Skripte zur Umwandlung Ihrer alten Authentifizierungsinformationen in das LDAP-Format.

Anmerkung

Um diese Skripte ausführen zu können, müssen Sie Perl auf Ihrem System installiert haben.

Zuerst müssen Sie die Datei `migrate_common.ph` an Ihre Domain anpassen. Die Standardwerte der Standard-DNS-Domain müssen ähnlich wie folgt geändert werden:

```
$DEFAULT_MAIL_DOMAIN = "example";
```

Die Standardannahme muss ebenfalls geändert werden von:

```
$DEFAULT_BASE =
"dc=example,dc=com";
```

Das Umwandeln einer Benutzerdatenbank in ein LDAP-Format fällt einer Gruppe von Umwandlungsskripten im gleichen Verzeichnis zu. Entscheiden Sie mit Hilfe von Tabelle 12-1, welches Skript zur Umwandlung der Benutzerdatenbank ausgeführt werden soll.

Führen Sie das Ihrem vorhandenen Name-Service entsprechende Skript aus.

Die Dateien `README` und `migration-tools.txt` im Verzeichnis `/usr/share/openldap/migration/` enthalten weitere Detailinformationen zum Umwandeln der Informationen.

Vorhandener Namensdienst	Wird LDAP ausgeführt?	Zu verwendendes Skript
`/etc` Klartext-Dateien	Ja	`migrate_all_online.sh`
`/etc` Klartext-Dateien	Nein	`migrate_all_offline.sh`
NetInfo	Ja	`migrate_all_netinfo_online.sh`
NetInfo	Nein	`migrate_all_netinfo_offline.sh`
NIS (YP)	Ja	`migrate_all_nis_online.sh`
NIS (YP)	Nein	`migrate_all_nis_offline.sh`

Tabelle 12-1. LDAP Umwandlungsskripte

12.8. Umwandeln von Verzeichnissen früherer Releases

Mit Beginn der Release von Red Hat Linux 9, benutzt OpenLDAP das *Berkeley DB* System von Sleepy Cat Software, als On-Disk Speicherformat. Frühere Versionen von OpenLDAP verwendeten den *GNU Database Manager* (*gdbm*). Aus diesem Grund sollten, vor einem Upgrade einer LDAP-Implementation auf Red Hat Enterprise Linux 3 von Red Hat Enterprise Linux 2.1 oder Red Hat Linux 7.x bis 8, diese Schritte durchgeführt werden:

1. Bevor Sie ein Upgrade des Betriebssystems durchführen, führen Sie den Befehl `/usr/sbin/slapcat -l ldif-Ausgabe` aus. Dieser gibt eine LDIF-Datei *`ldif-Ausgabe`* aus, die die Einträge aus dem LDAP-Verzeichnis enthält.
2. Führen Sie ein Upgrade des Betriebssystems durch und stellen Sie dabei sicher, dass Sie die Partition, die die LDIF-Datei enthält, nicht neu formatieren.
3. Importieren Sie das LDAP-Verzeichnis erneut zum aktuellen Berkeley DB Format, indem Sie den Befehl `/usr/sbin/slapadd -l ldif-output` ausführen.

Wichtig

Sollte ein LDAP-Verzeichnis nicht exportiert werden, bevor das Upgrade zu Red Hat Enterprise Linux 3 von Red Hat Enterprise Linux 2.1 oder Red Hat Linux 7.x bis 8 durchgeführt wird, benutzen Sie den Befehl `/usr/sbin/slapcat-gdbm -l ldif-output`, um das alte Verzeichnis zu extrahieren (*`ldif-output`* steht hierbei für den Dateinamen der LDIF-Ausgabe). Dieser Befehl erzeugt eine LDIF-Datei, die mit dem Befehl `slapadd` importiert werden kann.

12.8.1. Umwandeln der 1.x Verzeichnisse

Mit Red Hat Linux 7.1 beginnend, wurde das On-Disk Speicherformat vom `slapd` LDAP Server auf gdbm geändert. Wenn Sie LDAP von Red Hat Linux 7.0 oder früher aktualisieren, müssen Sie die existierenden LDAP-Verzeichnisse mit Hilfe des folgenden Befehls in eine LDIF-Datei exportieren:

```
ldbmcat -n > <ldif_file>
```

Geben Sie im obigen Befehl als <*`ldif_file`*> den Namen der Ausgabedatei ein. Geben Sie anschließend den folgenden Befehl ein, um die Datei zu importieren: 2.0:

```
slapadd -l <ldif_file>
```

Wichtig

Sie müssen root sein, um `/usr/sbin/slapadd` verwenden zu können. Der Verzeichnis-Server wird jedoch als Benutzer `ldap` ausgeführt. Der Verzeichnis-Server ist deshalb nicht in der Lage, Dateien, welche von `slapadd` erzeugt wurden, zu ändern. Um dieses Problem zu beheben, geben Sie den folgenden Befehl ein, nachdem Sie `slapadd` beendet haben:

```
chown -R ldap /var/lib/ldap
```

12.9. Zusätzliche Ressourcen

Es sind weitere, LDAP betreffende Informationen erhältlich. Konsultieren Sie bitte diese Quellen, insbesondere die OpenLDAP-Website und das LDAP HOWTO, ehe Sie LDAP auf Ihrem System konfigurieren.

12.9.1. Installierte Dokumentationen

- `/usr/share/docs/openldap-<Versionsnummer>` — Enthält ein allgemeines `README`-Dokument und sonstige Informationen.
- LDAP-bezogene man-Seiten — Es gibt eine Reihe von man-Seiten für die verschiedenen Applikationen und Konfigurationsdateien, die im Bezug zu LDAP stehen. Die Folgende, ist eine Liste einiger der wichtigeren man-Seiten.

  Client-Applikationen

  - `man ldapadd` — Beschreibt das Hinzufügen von Einträgen zum LDAP-Verzeichnis.
  - `man ldapdelete` — Beschreibt das Löschen von Einträgen aus dem LDAP-Verzeichnis.
  - `man ldapmodify` — Beschreibt das Bearbeiten von Einträgen im LDAP-Verzeichnis.
  - `man ldapsearch` — Beschreibt wie nach Einträgen im LDAP-Verzeichnis gesucht werden kann.
  - `man ldappasswd` — Beschreibt wie ein Passwort eines LDAP-Benutzers gesetzt oder geändert werden kann.

  Server-Applikationen

  - `man slapd` — Beschreibt zur Verfügung stehende Befehlszeilenoptionen für den LDAP-Server.
  - `man slurpd` — Beschreibt zur Verfügung stehende Befehlszeilenoptionen für den LDAP-Replication-Server.

  Administrative Applikationen

  - `man slapadd` — Beschreibt zur Verfügung stehende Befehlszeilenoptionen für dieses Tool, verwendet zum Hinzufügen von Einträgen zur `slapd` Datenbank.
  - `man slapcat` — Beschreibt zur Verfügung stehende Befehlszeilenoptionen für dieses Tool, verwendet zur Erzeugung einer LDIF-Datei von einer `slapd` Datenbank.
  - `man slapindex` — Beschreibt zur Verfügung stehende Befehlszeilenoptionen für dieses Tool, verwendet zur Erzeugung eines auf dem Inhalt einer `slapd` Datenbank basierenden Index.
  - `man slappasswd` — Beschreibt zur Verfügung stehende Befehlszeilenoptionen für dieses Tool, verwendet zur Erzeugung von Benutzerpasswörtern für LDAP-Verzeichnisse.

Konfigurationsdateien

- `man ldap.conf` — Beschreibt das Format der und die in der Konfigurationsdatei von LDAP-Clients verfügbaren Optionen.
- `man slapd.conf` — Beschreibt das Format und die Optionen, der sowohl von LDAP Server-Applikationen (`slapd` und `slurpd`), als auch von LDAP administrativen Tools (`slapadd`, `slapcat`, und `slapindex`) referenzierten Konfigurationsdatei.

12.9.2. Hilfreiche Websites

- http://www.openldap.org — Homepage des OpenLDAP-Projekts. Auf dieser Website finden Sie äußerst viele Informationen zum Konfigurieren von OpenLDAP.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — Ein älteres, aber immer noch relevantes LDAP-HOWTO.
- http://www.padl.com — Entwickler von `nss_ldap` und `pam_ldap`, neben vielen anderen hilfreichen LDAP-Tools.
- http://www.kingsmountain.com/ldapRoadmap.shtml — Jeff Hodges' LDAP Road Map enthält Links für verschiedene hilfreiche FAQs und aktuelle Neuigkeiten über das LDAP-Protokoll.
- http://www.newarchitectmag.com/archives/2000/05/wilcox/ — Ein hilfreicher Einblick in das Verwalten von Gruppen in LDAP.
- http://www.ldapman.org/articles — Artikel zur Einführung in LDAP einschließlich Methoden zur Erstellung eines Verzeichnisbaums und benutzerdefinierter Verzeichnis- strukturen.

12.9.3. Bücher zum Thema

- *Implementing LDAP* von Mark Wilcox; Wrox Press, Inc.
- *Understanding and Deploying LDAP Directory Services* von Tim Howes et al.; Macmillan Technical Publishing

III. Hinweis zur Sicherheit

Die Verwendung von sicheren Protokollen ist ein wichtiger Teil bei der Aufrechterhaltung der Systemintegrität. Dieser Abschnitt beschreibt kritische Werkzeuge, die für Benutzer-Authentifizierung, Netzwerk-Zugangskontrolle, sichere Netzwerkkommunikation und das Aufspüren von Eindringversuchen verwendet werden. Siehe *Red Hat Enterprise Linux Sicherheitshandbuch* für weitere Informationen zur Sicherung eines Red Hat Enterprise Linux Systems

Inhaltsverzeichnis

13. Pluggable Authentication Modules (PAM) 201
14. TCP Wrappers und `xinetd` 211
15. `iptables` 227
16. Kerberos 241
17. SSH-Protokoll 251

Kapitel 13.

Pluggable Authentication Modules (PAM)

Programme, die Benutzern Zugriff zu einem System gewähren, überprüfen die Identität der Benutzer durch einen Prozess, der *Authentifizierung* genannt wird. Historisch haben alle diese Programme ihren eigenen Weg, die Authentifizierung durchzuführen. Unter Red Hat Enterprise Linux sind viele dieser Programme dafür konfiguriert, einen zentralisierten Authentifizierungsprozess zu benutzen, der *Pluggable Authentication Modules* (*PAM*) genannt wird.

PAM benutzt eine auswechselbare, modulare Architektur, welche dem System-Administrator einen hohen Grad an Flexibilität beim Einstellen der Authentifizierungsregeln des Systems bereit stellt.

Es ist kaum notwendig, die Standard PAM Konfigurationsdateien für eine Applikation, welche PAM verwendet, zu ändern. Hin und wieder kann es allerdings notwendig werden, eine PAM Konfigurationsdatei zu ändern. Da eine falsche Einstellung in der PAM Konfigurationsdatei die Systemsicherheit kompromitieren kann, sollten Sie mit der Struktur der Konfigurationsdateien von PAM vertraut sein, bevor Sie eventuelle Änderungen vornehmen (weitere Informationen finden Sie unter Abschnitt 13.3).

13.1. Vorteile von PAM

PAM bietet die folgenden Vorteile:

- Es stellt ein gemeinsames Authentifikationsschema bereit, das für viele verschiedene Anwendungen verwendet werden kann.
- Es erlaubt große Flexibilität und Kontrolle der Authentifizierung für Administratoren und Entwickler von Anwendungen.
- Es erlaubt Anwendungsentwicklern ihr Programm nicht speziell für die Verwendung bestimmter Authentifikationsschemata entwickeln zu müssen.

13.2. PAM-Konfigurationsdateien

Die PAM-Konfigurationsdateien sind im Verzeichnis `/etc/pam.d/` enthalten. In früheren Versionen von PAM wurde die Datei `/etc/pam.conf` verwendet, die aber künftig nicht mehr verwendet wird. Die Datei `pam.conf` wird nur eingelesen, wenn das Verzeichnis `/etc/pam.d/` nicht existiert.

13.2.1. PAM Servicedateien

Für Applikationen oder *Services*, welche PAM verwenden, besteht eine Datei im Verzeichnis `/etc/pam.d/`. Jede dieser Dateien ist nach dem Service benannt, für welchen diese den Zugriff kontrolliert.

Es ist dem PAM verwendenden Programm überlassen seinen Servicenamen zu bestimmen und die entsprechende PAM Konfigurationsdatei im Verzeichnis `/etc/pam.d/` abzulegen. Das `login` Program, zum Beispiel, bestimmt seinen Servicenamen als `/etc/pam.d/login`.

13.3. Format der PAM Konfigurationsdatei

Jede PAM Konfigurationsdatei enthält eine Gruppe von Anweisungen, welche wie folgt formattiert sind:

<module interface> *<control flag>* *<module name>* *<module arguments>*

Jedes dieser Elemente ist in den folgenden Abschnitten erklärt.

13.3.1. Modul-Schnittstellen

Es gibt vier Typen von Modul-Schnittstellen, welche den unterschiedlichen Aspekten des Authentifizierungsprozesses entsprechen:

- `auth` — Diese Modulschnittstelle authentifiziertdie Verwendung. Sie, zum Beispiel, erfragt und überprüft das Passwort und stellt Berechtigungsmerkmale, wie z.B. Mitgliedschaft in einer Gruppe oder Kerberos-Tickets, ein.
- `account` — Diese Modulschnittstelle stellt sicher, dass der Zugriff erlaubt ist. Zum Beispiel können sie prüfen, ob der Account abgelaufen ist, oder ob der Benutzer zur Anmeldung um diese Uhrzeit zugelassen ist.
- `password` — Diese Modulschnittstelle wird zur Einstellung des Passworts verwendet.
- `session` — Diese Modulschnittstelle wird, nachdem der Benutzer authentifiziert wurde, dazu verwendet, dessen Session zu verwalten. Das Modul kann auch zusätzliche, für den Zugriff benötigte Tasks durchführen, wie beispielsweise das Mounten des Home-Verzeichnisses des Benutzers oder die Aktivierung seiner Mailbox.

Anmerkung

Ein einzelnes Modul kann jeglichen, oder alle der o.g. Modul-Schnittstellen ansprechen. Zum Beispiel `pam_unix.so` besitzt Komponenten, die alle vier Modularten ansprechen.

In einer PAM Konfigurationsdatei wird als Erstes die Modul-Schnittstelle bestimmt. Eine solche typische Zeile in einer Konfiguration könnte wie folgt aussehen:

```
auth      required  pam_unix.so
```

Dies weist PAM an, die `auth`-Schnittstelle des `pam_unix.so` Moduls zu verwenden.

13.3.1.1. Modul-Schnittstellen stapeln

Anweisungen der Modul-Schnittstellen können *gestapelt* werden, so dass mehrere Module zu einem Zweck verwendet werden können. Deshalb ist die Reihenfolge in der die Module aufgelistet werden für den Authentifikationsprozess sehr wichtig.

Das Stapeln macht es dem Administrator einfacher, zu erkennen, dass bereits einige Voraussetzungen erfüllt sind, bevor die Benutzerauthentifizierung stattgefunden hat. Zum Beispiel verwendet `rlogin` in der Regel fünf gestapelte `auth` Module, wie in der PAM-Konfigurations- datei zu sehen:

```
auth       required     pam_nologin.so
auth       required     pam_securetty.so
auth       required     pam_env.so
auth       sufficient   pam_rhosts_auth.so
auth       required     pam_stack.so service=system-auth
```

Bevor `rlogin` ausgeführt werden kann, stellt PAM fest, dass die Datei `/etc/nologin` nicht existiert, dass niemandversucht, sich von einem Remote-Rechner über eine unverschlüsselte Netzwerkverbindung als Root anzumelden und dass alle Umgebungsvariablen geladen werden können. Wenn die

`rhosts` -Authentifizierung erfolgreich ist, kann die Verbindung zugelassen werden. Ist die Authentifizierung nicht erfolgreich, wird zur Standardauthentifizierung mit Passwort übergegangen.

13.3.2. Steuer-Flags

Alle PAM-Module erstellen bei einer Überprüfung Fehler- oder Erfolgsmeldungen. Die Steuer-Flags geben PAM an, was mit diesen Ergebnissen geschehen soll. Während Module in einer bestimmten Reihenfolge gestapelt werden können, können Sie mit den Steuer-Flags einstellen, wie wichtig der Erfolg oder das Fehlschlagen des entsprechenden Moduls für die Authentifizierung des gesamten Service ist.

Es gibt vier vordefinierte Steuer-Flags:

- `required` — Solche Module müssen erfolgreich überprüft werden, bevor die Authentifizierung erfolgen kann. Wenn bei einem `required` Modul Fehler auftreten, wird der Benutzer darüber informiert, sobald auch alle anderen Module, welche die gleiche Schnittstelle referenzieren überprüft wurden.
- `requisite` — Solche Module müssen ebenfalls überprüft werden, bevor die Authentifizierung erfolgreich sein kann. Wenn bei einem `requisite` Modul Fehler auftreten, wird der Benutzer hierüber sofort informiert. Diese Mitteilung zeigt das erste fehlerhafte `required` *oder* `requisite` Modul an.
- `sufficient` — Bei solchen Modulen werden Fehler ignoriert. Wenn ein `sufficient` Modul jedoch erfolgreich überprüft wurde, und kein `required` Modul fehlschlägt, werden keine weiteren Überprüfungen dieser Modul-Schnittstelle benötigt und diese wird erfolgreich authentifiziert.
- `optional` — Solche Module sind für die erfolgreiche oder fehlgeschlagene Authentifizierung dieser Modul-Schnittstelle nicht von Bedeutung. Diese werden nur dann wichtig, wenn kein anderes Modul dieser Modul-Schnittstelle erfolgreich war oder fehlgeschlagen ist.

Wichtig

Die Reihenfolge in welcher `required` Module aufgerufen werden spielt keine Rolle. Bei den Steuer-Flags `sufficient` und `requisite` ist die Reihenfolge allerdings wichtig.

Eine neuere Steuer-Flag Syntax mit immer mehr Kontrollmöglichkeiten steht nun für PAM zur Verfügung. Mehr Informationen über diese neue Syntax finden Sie in den PAM-Dokumentationen im Verzeichnis `/usr/share/doc/pam-`*`version-number`*`/` (wobei <*`version-number`*> die Versionsnummer von PAM ist).

13.3.3. Modulname

Der Modulname liefert PAM den Namen des Pluggable Moduls, das die angegebene Modulschnittstelle enthält. Unter älteren Versionen von Red Hat Enterprise Linux wurde der vollständige Pfad zum Modul in der PAM-Konfigurationsdatei angegeben, wie z.B. `/lib/security/pam_stack.so`. Seit dem Aufkommen von Multilib-Systemen, die 64-bit PAM Module im Verzeichnis `/lib64/security/` speichern, wird der Verzeichnisname jedoch weggelassen, da die Applikation zur richtigen Version von `libpam` verbunden ist, die die richtige Version des Moduls feststellen kann.

13.3.4. Modul-Argumente

PAM verwendet Argumente, um während der Authentifizierung Informationen über eine bestimmte Modul-Schnittstelle einem "Pluggable Module" zu übermitteln.

Zum Beispiel verwendet das Modul `pam_userdb.so` versteckte Dateien aus der Berkeley DB-Datei, um den Benutzer zu authentifizieren. Berkeley DB ist eine in vielen Anwendungen eingebundenes Open-Source Datenbank-System. Das Modul verwendet ein `db` Argument, welches die von Berkeley DB für den angeforderten Service zu verwendende Datenbank angibt.

Eine typische `pam_userdb.so` Zeile in einer PAM- Konfigurationsdatei sieht wie folgt aus:

```
auth      required  pam_userdb.so db=<path-to-file>
```

Im vorangegangenen Beispiel ersetzen Sie *<path-to-file>* mit dem vollständigen Pfad der Berkeley DB Datenbank-Datei.

Ungültige Argumente werden ignoriert und wirken sich auch nicht auf den Erfolg oder Misserfolg eines PAM-Moduls aus. Wenn ein ungültiges Argument auftaucht, erscheint jedoch normalerweise eine Fehlermeldung in `/var/log/messages`.

13.4. Beispiele für PAM-Konfigurationsdateien

Eine Konfigurationsdatei einer PAM-Anwendung sieht z.B. wie folgt aus:

```
#%PAM-1.0
auth      required  pam_securetty.so
auth      required  pam_unix.so shadow nullok
auth      required  pam_nologin.so
account   required  pam_unix.so
password  required  pam_cracklib.so retry=3
password  required  pam_unix.so shadow nullok use_authtok
session   required  pam_unix.so
```

Die erste Zeile ist ein Kommentar, was durch das Hash-Zeichen (`#`) am Anfang der Zeile erkenntlich ist.

Die Zeilen zwei bis vier stellen drei Module in den Stack für die Authentifizierung bei der Anmeldung.

```
auth      required  pam_securetty.so
```

Wenn der Benutzer sich als Root anzumelden versucht, stellt dieses Modul sicher, dass das Terminal, an dem er sich anmeldet, in der Datei `/etc/securetty` aufgeführt ist, *falls* solch eine Datei existiert.

```
auth      required  pam_unix.so shadow nullok
```

Dieses Modul fragt den Benutzer nach einem Passwort und überprüft dieses Passwort anhand der in `/etc/passwd` und, falls vorhanden, in `/etc/shadow` gespeicherten Informationen. Das Modul `pam_unix.so` erkennt gespeicherte Shadow-Passwörter und verwendet sie zur Authentifizierung von Benutzern. Im Abschnitt 6.5 finden Sie weitere Informationen.

Das Argument `nullok` weist das Modul `pam_unix.so` an, ein leeres Passwort zuzulassen.

```
auth      required  pam_nologin.so
```

Das ist der letzte Schritt der Authentifizierung. Es wird geprüft, ob die Datei `/etc/nologin` existiert. Falls `nologin` existiert, und der Benutzer nicht als Root angemeldet ist, schlägt die Authentifizierung fehl.

Anmerkung

In diesem Beispiel werden alle drei `auth` Module überprüft, auch wenn schon beim ersten `auth` Modul Fehler auftreten. Der Grund dafür ist: wenn ein Benutzer weiß, weshalb seine Authentifizierung abgelehnt wurde, ist es für ihn einfacher, diese zu umgehen.

```
account   required  pam_unix.so
```

Dieses Modul übernimmt jegliche Prüfung des Benutzeraccounts. Wenn z.B. Shadow-Passwörter aktiviert worden sind, überprüft das Modul `pam_unix.so`, ob der Account abgelaufen ist oder ob der Benutzer keine Passwortänderung vorgenommen hat und die Nachfrist für eine Änderung abgelaufen ist.

```
password  required  pam_cracklib.so retry=3
```

Ist ein Passwort abgelaufen, fordert die Passwort-Komponente des `pam_cracklib.so` Moduls zur Eingabe eines neuen Passworts auf. Zusätzlich wird das neue Passwort getestet, um festzustellen, ob es einfach durch ein Wörterbuch-basiertes Programm zum Erkennen von Passwörtern erkannt werden kann. Schlägt der Test einmal fehl, hat der Benutzer aufgrund des Arguments `retry=3` zwei weitere Möglichkeiten, ein besseres Passwort zu erstellen.

```
password  required  pam_unix.so shadow nullok use_authtok
```

Diese Zeile legt fest, dass bei einer Änderung des Benutzer-Passworts durch das Programm die `password` Komponente des `pam_unix.so` Moduls verwendet wird. Das passiert nur, wenn der Teil `auth` des `pam_unix.so` Moduls bestimmt, dass das Passwort geändert werden muss.

Das Argument `shadow` teilt dem Modul mit, beim Updaten eines Benutzer-Passworts ein Shadow-Passwort zu erstellen.

Das Argument `nullok` weist das Modul an, dem Benutzer zu erlauben sein Passwort *von* einem leeren Passwort zu ändern. Andernfalls wird ein Null-Passwort als Account-Sperre betrachtet.

Das letzte Argument dieser Zeile ist `use_authtok` und ein gutes Beispiel für die Wichtigkeit der Reihenfolge beim Stapeln von PAM-Modulen. Dieses Argument weist das Modul an, den Benutzer nicht zur Eingabe eines neuen Passworts aufzufordern. Stattdessen wird jedes Passwort akzeptiert, das von vorherigen Passwort-Modulen verwendet wurde. Auf diese Weise müssen allen neuen Passwörter den `pam_cracklib.so` Test für sichere Passwörter durchlaufen, bevor sie akzepiert werden.

```
session required pam_unix.so
```

Die letzte Zeile gibt an, dass das Modul `pam_unix.so` für die Verwaltung der Sitzung verwendet werden soll. Dieses Modul protokolliert bei jedem Start und Ende einer Sitzung den Benutzernamen und den Service-Typ in die Datei `/var/log/messages`. Wenn Sie weitere Funktionen benötigen, kann es durch das Stapeln mit anderen Sitzungsmodulen ergänzt werden.

Die nächste Beispielkonfigurationsdatei erläutert das `auth` Modulstapeln für den `rlogin` Dienst.

```
#%PAM-1.0
auth       required     pam_nologin.so
auth       required     pam_securetty.so
auth       required     pam_env.so
auth       sufficient   pam_rhosts_auth.so
auth       required     pam_stack.so service=system-auth
```

Zunächst überprüft `pam_nologin.so`, ob `/etc/nologin` existiert. Ist dies der Fall, kann sich niemand anmelden, mit Ausnahme des Rootbenutzers.

```
auth       required     pam_securetty.so
```

Anschließend verhindert `pam_securetty.so`, dass Root-Anmeldungen auf unsicheren Terminals vorgenommen werden können. Damit werden praktisch alle Root-Anmeldungen über `rlogin` aus Sicherheitsgründen verhindert.

Tipp

Um sich als Root von einem Remote-Rechner aus anzumelden, benutzen Sie OpenSSH. Für mehr Informationen zum SSH Protokoll sehen Sie Kapitel 17.

```
auth       required     pam_env.so
```

Diese Zeile lädt das Modul `pam_env.so`, das die in `/etc/security/pam_env.conf` angegebenen Umgebungsvariablen festlegt.

```
auth       sufficient   pam_rhosts_auth.so
```

Das `pam_rhosts_auth.so` Modul authentifiziert den Benutzer unter Verwendung von `.rhosts` im Hauptverzeichnis des Benutzers. Sollte dies erfolgreich sein, wird PAM die Authentifizierung als erfolgreich ansehen. Sollte `pam_rhosts_auth.so` fehlschlagen, wird dieser Versuch der Authentifizierung ignoriert.

```
auth       required     pam_stack.so service=system-auth
```

Wenn die Authentifizierung des Benutzers durch `pam_rhosts_auth.so` gescheitert ist, führt das `pam_stack.so` Modul eine normale Passwort-Authentifizierung durch.

Das Argument `service=system-auth` bedeutet, dass der Benutzer die PAM-Konfiguration zur System- Authentifizierung in `/etc/pam.d/system-auth` durchlaufen muss.

Tipp

Wenn Sie den Prompt beim Eingeben des Passworts nicht anzeigen möchten, nachdem die `securetty` Prüfung fehlgeschlagen ist, können Sie das `pam_securetty.so` Modul von `required` in `requisite` ändern.

13.5. Module erstellen

Es können jederzeit neue PAM-Module hinzugefügt werden. PAM-kompatible Anwendungen können dann so angepasst werden, dass diese Module verwendet werden können. Falls Sie z.B. über ein Rechensystem für Einmal-Passwörter verfügen und festlegen können, dass es von einem PAM-Modul unterstützt werden soll, sind PAM-kompatible Programme in der Lage, das neue Modul zu verwenden und mit dem neuen Rechensystem für Einmal-Passwörter zu arbeiten, ohne dass es neu kompiliert oder anderweitig modifiziert werden müsste. Das ist sehr nützlich, da Sie dadurch sehr schnell Authentifizierungsmethoden mit verschiedenen Programmen vermischen und vergleichen sowie testen können, ohne die Programme neu zu kompilieren.

Dokumentationen über das Schreiben von Modulen finden Sie im Verzeichnis `/usr/share/doc/pam-<version-number>/` (wobei *<version-number>* die Versionsnummer von PAM ist).

13.6. PAM und Administrative-Credential-Caching

Eine Reihe grafischer Verwaltungstools unter Red Hat Enterprise Linux geben Benutzern erweiterte Rechte über das Modul `pam_timestamp.so` für eine Zeitdauer von 5 Minuten. Es ist wichtig zu verstehen, wie dieser Mechanismus funktioniert, denn wenn ein Benutzer sich vom Terminal entfernt, während `pam_timestamp.so` ausgeführt wird, ist der Rechner offen für Manipulationen von jedem mit physischem Zugang zur Konsole.

Unter dem PAM Timestamp-Scheme, wird die grafische Verwaltungsapplikation beim Starten den Benutzer nach dem Root-Passwort fragen. Nach der Authentifizierung, erzeugt das `pam_timestamp.so`-Modul eine Timestamp-Datei im Verzeichnis `/var/run/sudo/`. Sollte diese Datei bereits existieren, werden andere grafische Verwaltungstools nicht nach dem Passwort fragen. Das `pam_timestamp.so`-Modul wird anstelle die Timestamp-Datei aktualisieren; wobei dem Benutzer fünf Minuten freier administrativer Zugriff gewährt werden.

Das Bestehen der Timestamp-Datei wird durch ein Authetifizierungssymbol in der Notification-Area des Panels angezeigt. Folgend ist eine Illustration des Authetifizierungssymbols.

Abbildung 13-1. Das Authentication Icon

13.6.1. Entferne die Timestamp-Datei

Es wird empfohlen, dass bevor Sie sich von einer Konsole entfernen, an der PAM läuft, die Timestamp-Datei gelöscht wird. Um dies innerhalb der grafischen Umgebung zu tun, klicken Sie auf das Authetifizierungssymbol im Panel. Wenn das Dialog-Fenster erscheint, klicken Sie den Button **Forget Authorization**.

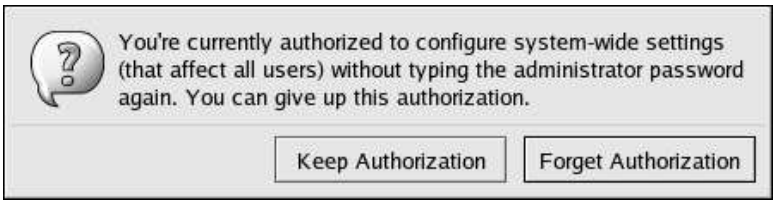
You're currently authorized to configure system-wide settings (that affect all users) without typing the administrator password again. You can give up this authorization.
Keep Authorization
Forget Authorization

Abbildung 13-2. Authentifizierungssymbol Dialog

Wenn von einem Remote-System aus mit `ssh` angemeldet, benutzen Sie den Befehl `/sbin/pam_timestamp_check -k root`, um die Timestap-Datei zu löschen.

Anmerkung

Nur der Benutzer, der ursprünglich das`pam_timestamp.so`-Modul aufgerufen hat, kann den Befehl `/sbin/pam_timestamp_check` verwenden. Melden Sie sich nicht als root an, um diesen Befehl auszuführen.

Zu Informationen zum Löschen der Timestamp-Datei mittels`pam_timestamp_check`, sehen Sie die man-Seiten von`pam_timestamp_check`.

13.6.2. Allgemeine `pam_timestamp` Anweisungen

Das `pam_timestamp.so` Modul akzeptiert verschiedene Anweisungen. Folgend sind die zwei am häufigsten verwendeten angegeben:

- `timestamp_timeout` — Die Anzahl der Sekunden, während denen die Timestap-Datei gültig ist. Der Standardwert ist 300 Sekunden (fünf Minuten).
- `timestampdir` — Gibt das Verzeichnis an, in dem die Timestamp-Datei gespeichert ist. Der Standardwert ist `/var/run/sudo`.

Für weitere Informationen zur Kontrolle des `pam_timestamp.so`-Moduls, sehen Sie Abschnitt 13.8.1.

13.7. PAM und Besitzrechte von Geräten

Red Hat Enterprise Linux erlaubt es dem ersten Benutzer mithilfe des PAM-Moduls `pam_console.so`, sich in der Konsole des Computers anzumelden, sowie das Bearbeiten von Geräten und das Ausführen von Tasks, die normalerweise für Root-Benutzer reserviert sind.

13.7.1. Besitzrechte von Geräten

Wenn sich ein Benutzer unter Red Hat Enterprise Linux in einem Computer anmeldet, wird das `pam_console.so` Modul durch `login` oder die grafischen Anmeldeprogramme **gdm** und **kdm** aufgerufen. Ist dieser Benutzer der erste Benutzer, der sich in der physischen Konsole anmeldet — *Konsolen-Benutzer* genannt — bewilligt das Modul dem Benutzer das Besitzrecht einer ganzen Reihe von Geräten, die normalerweise im Besitz von Root sind. Der Konsolen-Benutzer besitzt diese Geräte solange, bis die letzte lokale Sitzung für diesen Benutzer beendet ist. Sobald sich der Benutzer abgemeldet hat, kehrt das Besitzrecht auf seinen Standardwert zurück.

Es sind alle Geräte betroffen, nicht nur Soundkarten, Disketten-Laufwerke und CD-ROM Laufwerke.

Dadurch hat der lokale Benutzer die Möglichkeit, diese Geräte zu bearbeiten, ohne als Root angemeldet zu sein, was allgemeine Tasks für den Konsolen-Benutzer vereinfacht.

Die Liste von Geräten, die von `pam_console.so` kontrolliert werden können vom Administrator in der Datei `/etc/security/console.perms` bearbeitet werden.

Warnung

Wenn die Konfigurationsdatei des **gdm**, **kdm**, oder **xdm** Display-Manager geändert wurde, um Remote-Benutzern den Zugriff zu gewähren, *und* der Host ist zur Ausführung in Runlevel 5 konfiguriert, dann wird empfohlen, die `<console>` und `<xconsole>`-Anweisungen in der Datei `/etc/security/console.perms` auf folgende Werte zu ändern:

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]* :0\.[0-9] :0
<xconsole>=:0\.[0-9] :0
```

Dies wird Remote-Benutzer davon abhalten, Zugriff auf Geräte und Applikationen höherer Sicherheitsstufe zu gelangen.

Wenn die Konfigurationsdatei des **gdm**, **kdm**, oder **xdm** Display-Manager geändert wurde, um Remote-Benutzern den Zugriff zu gewähren, *und* der Host ist zur Ausführung in Runlevel 5 konfiguriert, dann wird empfohlen, die `<console>` und `<xconsole>`-Anweisungen auf folgende Werte zu ändern:

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]*
```

13.7.2. Zugriff zu Applikationen

Der Konsolen-Benutzer hat die Möglichkeit, mithilfe einer Datei, die den Befehlsnamen im Verzeichnis `/etc/security/console.apps/` enthält, zu bestimmten Programm Zugriff zu erhalten.

Eine wichtige Gruppe von Applikationen, zu denen der Konsolen-Benutzer Zugriff hat, sind folgende drei Programme zum Abschalten und Neubooten des Systems:

- `/sbin/halt`
- `/sbin/reboot`
- `/sbin/poweroff`

Da diese Programme PAM-kompatible Applikationen sind, benötigen sie das `pam_console.so` Modul.

Für weitere Informationen, sehen Sie Abschnitt 13.8.1.

13.8. Zusätzliche Ressourcen

Folgend finden Sie eine Aufstellung von Informationsquellen zur Verwendung und Konfiguration von PAM. Zusätzlich zu diesen Quellen sollten Sie sich mit den PAM-Konfigurationsdateien in Ihrem System vertraut machen, um deren Aufbau besser zu verstehen.

13.8.1. Installierte Dokumentationen

- PAM-bezogene man-Seiten — Es gibt eine Reihe von man-Seiten für die verschiedenen Applikationen und Konfigurationsdateien, die im Bezug zu PAM stehen. Folgend ist eine Liste der wichtigeren man-Seiten.

  Konfigurationsdateien

  - `man pam` — Eine gute Einführung in PAM, einschließlich der Struktur und der Funktion von PAM Konfigurationsdateien. Bitte beachten Sie, das obwohl diese man-Seiten die Datei `/etc/pam.conf` behandeln, die tatsächlichen Konfigurationsdateien für PAM in Red Hat Enterprise Linux sind im Verzeichnis `/etc/pam.d/`.
  - `man pam_console` — Beschreibt die Funktion des `pam_console.so`-Moduls. Beschreibt auch die entsprechende Syntax eines Eintrags in der PAM Konfigurationsdatei.
  - `man console.apps` — Beschreibt das Format und die verfügbaren Optionen der Konfigurationsdatei `/etc/security/console.apps`, die festlegt, auf welche Applikationen der durch PAM zugewiesenen Konsolenbenutzer zugreifen kann.
  - `man console.perms` — Beschreibt das Format und die verfügbaren Optionen der Konfigurationsdatei `/etc/security/console.perms`, die die Zugriffsrechte des durch PAM zugewiesenen Konsolenbenutzers festlegt.
  - `man pam_timestamp` — Beschreibt das`pam_timestamp.so`-Modul.

- `/usr/share/doc/pam-<version-number>` — Enthält einen *System Administrators' Guide*, ein *Module Writers' Manual* und ein *Application Developers' Manual* sowie eine Kopie des PAM Standards, DCE-RFC 86.0 (`<version-number>` steht hierbei für die Versionsnummer von PAM).
- `/usr/share/doc/pam-<version-number>/txts/README.pam_timestamp` — Enthält Informationen über das `pam_timestamp.so` PAM-Module (wobei `<version-number>` die Versionsnummer von PAM ist).

13.8.2. Hilfreiche Websites

- http://www.kernel.org/pub/linux/libs/pam/ — Die wichtigste Website für Linux-PAM. Sie enthält Informationen über die verschiedenen PAM-Module und Anwendungen, die verwendet oder entwickelt werden, sowie FAQ und zusätzliche Dokumentationen über PAM.

Kapitel 14.

TCP Wrappers und `xinetd`

Die Kontrolle des Zugriffs zu Netzwerk-Services ist eine der wichtigsten Sicherheitsaufgaben, denen sich der Administrator stellen muss. Glücklicherweise gibt es unter Red Hat Enterprise Linux eine Reihe von Tools, welche genau dies tun. Eine `iptables`-basierte Firewall, zum Beispiel, filtert alle unerwünschten Netzwerk-Pakete im Netzwerk-Stack des Kernel heraus. Für Netzwerk-Services, welche davon Verwendung machen, fügt *TCP Wrappers* eine zusätzliche Schutzschicht hinzu, indem dieser definiert, welchen Hosts es erlaubt ist zu "*wrapped*" Netzwerk-Services zu verbinden, und welchen nicht. Einer dieser "wrapped" Netzwerk-Services ist `xinetd` *Super-Server*. Dieser Service wird Super-Server genannt, da dieser Verbindungen zu einem Subnet von Netzwerk-Services kontrolliert und Zugriffskontrolle weiter feinabstimmt.

Abbildung 14-1 ist eine grundlegende Illustration welche zeigt, wie diese Tools zusammen arbeiten um Netzwerk-Services zu schützen.

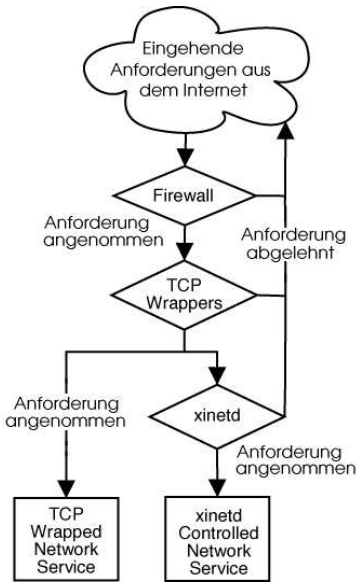

Abbildung 14-1. Zugriffskontrolle zu Netzwerk-Services

Dieses Kapitel beschäftigt sich mit der Rolle von TCP Wrappers und `xinetd` in der Zugriffskontrolle zu Netzwerk-Services und in wie diese Tools verwendet werden können um das Management von sowohl Logging, als auch Verwendbarkeit zu verbessern. Für eine Diskussion der Verbindung von Firewall und `iptables`, siehe Kapitel 15.

14.1. TCP Wrappers

Das TCP Wrappers Paket (`tcp_wrappers`) ist standardmäßig installiert und stellt Host-basierte Zugriffskontrolle zu Netzwerk-Services bereit. Die wichtigste Komponente in diesem Paket ist die

/usr/lib/libwrap.a-Bibliothek. In allgemeinen Begriffen, ist ein "TCP wrapped" Service einer, der gegen die libwrap.a-Bibliothek kompiliert wurde.

Wenn ein Verbindungsversuch zu einem "TCP wrapped" Service eingeleitet wird, wird der Service zuerst die *Hosts-Zugriffs*-Dateien (/etc/hosts.allow und /etc/hosts.deny) untersuchen, um festzustellen, ob der Client-Host erlaubt ist zu verbinden. Dieser wird dann den syslog-Daemon (syslogd) verwenden, um den Namen des anfordernden Hosts und Service entweder zu /var/log/secure oder zu /var/log/messages zu schreiben.

Wenn es einem Client-Host erlaubt ist zu verbinden, gibt TCP Wrapper die Kontrolle über die Verbindung zum angeforderten Service und wird nicht mehr in die Kommunikation zwischen Client-Host und Server eingreifen.

Zusätzlich zu Zugriffskontrolle und Logging, TCP Wrapper kann Befehle aktivieren um mit dem Client zu interagieren, bevor er die Kontrolle der Verbindung zum angeforderten Netzwerk-Service übergibt oder diesen ablehnt.

Da TCP Wrapper ein wertvoller Zusatz zum Arsenal jeden Administrators Sicherheits-Tools sind, sind die meisten Netzwerk-Services unter Red Hat Enterprise Linux gegen die libwrap.a gebunden. Einige dieser Anwendungen sind /usr/sbin/sshd, /usr/sbin/sendmail und /usr/sbin/xinetd.

Anmerkung

Um festzustellen, ob die Binärdatei eines Netzwerk-Service gegen libwrap.a gebunden ist, geben Sie den folgenden Befehl als root ein:

```
strings -f <binary-name> | grep hosts_access
```

Ersetzen Sie <*binary-name*> mit dem Namen der Binärdatei des Netzwerk-Service.

Wenn eine Anfrage beantwortet wird, dann ist der Netzwerk-Service *nicht* gegen libwrap.a gebunden.

14.1.1. Vorteile eines TCP Wrappers

TCP Wrappers bietet zwei grundlegende Vorteile im Vergleich zu anderen Kontrollmethoden für Netzwerkdienste:

- *Der sich verbindende Client bemerkt den Einsatz von TCP Wrappers nicht* — Zugelassene Benutzer bemerken keinen Unterschied und Angreifer erhalten niemals zusätzliche Informationen über den Grund dafür, warum ihr Verbindungsversuch fehlgeschlagen ist.
- *Zentralisiertes Management von mehreren Protokollen* — TCP Wrappers arbeiten unabhängig vom Netzwerkdienst, den sie schützen. Dies erlaubt es mehreren Server-Applikationen sich eine gemeinsame Gruppe von Konfigurationsdateien zu teilen, was ein vereinfachtes Management zur Folge hat.

14.2. TCP Wrappers Konfigurationsdateien

Um zu bestimmen, ob es einer Client-Maschine erlaubt ist, zu einem gewissen Service zu verbinden, verwenden TCP Wrappers die folgenden zwei Dateien, die auch Hosts-Zugriffsdateien gennant werden:

- /etc/hosts.allow

- `/etc/hosts.deny`

Wenn ein Verbindungsversuch zu einem "TCP wrapped" Service eingeleitet wird, wird der Service folgende Schritte durchführen:

1. *Der Service wird zuerst `/etc/hosts.allow` untersuchen.* — Der "TCP wrapped" Service arbeitet die Datei `/etc/hosts.allow` sequentiell ab, und wendet die erste für diesen Service angegebene Regel an. Sollte dieser eine solche Regel finden, erlaubt dieser die Verbindung. Wenn nicht, wird dieser zum Schritt 2 übergehen.
2. *Der Service untersucht `/etc/hosts.deny`.* — Der "TCP wrapped" Service arbeitet die Datei `/etc/hosts.deny` sequentiell ab. Sollte es eine entsprechende Regel finden, wird die Verbindung abgelehnt. Wenn nicht, wird die Verbindung erlaubt.

Die folgenden Punkte sind wichtig, wenn TCP Wrappers verwendet werden um Netzwerk-Services zu schützen:

- Da Zugriffsregeln in `hosts.allow` zuerst angewendet werden, haben diese Vorrang vor den Regeln in `hosts.deny`. Sollte der Zugriff zu einem Service in `hosts.allow` erlaubt sein, wird jegliche Regel in `hosts.deny`, welche den Zugriff verbietet, ignoriert.
- Da alle Regeln von oben nach unten abgearbeitet werden, wird lediglich die erste Regel für einen gegebenen Service angewendet, weswegen die Reihenfolge der Regeln sehr wichtig ist.
- Sollte keine Regel für einen gegebenen Service gefunden werden, in keiner der beiden Dateien, so wird der Zugriff zu diesem Service gewährt.
- "TCP wrapped" Services speichern Regeln für die Hosts-Zugriffsdateien nicht zwischen, jegliche Änderungen zu `hosts.allow` oder `hosts.deny` treten deswegen sofort in Kraft.

Warnung

Sollte die letzte Zeile einer Hosts-Zugriffsdatei keine Leerzeile sein (eine Leerzeile enthält lediglich ein Newline-Zeichen, und wurde durch Drücken der [Enter]-Taste erzeugt), wird die letzte Regel in der Datei nicht richtig abgearbeitet, und ein Fehler wird entweder nach `/var/log/messages` oder `/var/log/secure` geschrieben. Dies ist auch der Fall für Regelzeilen, welche auf mehrere Zeilen aufgeteilt werden, ohne den Backslash zu benutzen. Das folgende Beispiel zeigt den wichtigsten Teil einer Log-Meldung für eine durch genannte Gründe fehlerhafte Regel:

```
warning: /etc/hosts.allow, line 20: missing newline or line too long
```

14.2.1. Formatieren von Zugriffsregeln

Das Format der beiden Dateien `/etc/hosts.allow` und `/etc/hosts.deny` ist gleich. Leere Zeilen oder Zeilen, die mit dem Zeichen (`#`) beginnen, werden nicht berücksichtigt. Jede Regel muss auf einer neuen Zeile beginnen.

Jede Regel verwendet folgendes grundlegende Format, um den Zugriff zu Netzwerk-Services zu kontrollieren:

```
<daemon list>: <client list> [: <option>: <option>: ...]
```

- *<daemon list>* — Eine durch Kommas getrennte Liste von Prozessnamen (*nicht* Service-Namen) oder dem `ALLE` *Wildcard* (siehe Abschnitt 14.2.1.1). Die Daemon-Liste akzeptiert auch *Operatoren*, in Abschnitt 14.2.1.4 aufgelistet, um größere Flexibilität zu gewähren.

- <client list> — Eine durch Kommas getrennte Liste von Hostnamen, Host IP-Adressen, speziellen *Patterns* (siehe Abschnitt 14.2.1.2), oder speziellen Wildcards (siehe Abschnitt 14.2.1.1), welche die von dieser Regel betroffenen Hosts identifizieren. Die Client-Liste akzeptiert auch Operatoren, wie in Abschnitt 14.2.1.4 aufgelistet, um größere Flexibilität zu gewähren.
- <option> — Eine optionale Aktion oder durch Doppelpunkte getrennte Liste von Aktionen, welche ausgeführt werden, wenn eine Regel angewendet wird. Option-Felder unterstützen *Expansionen* (siehe Abschnitt 14.2.2.4), und können verwendet werden, um Shell-Befehle auszuführen, Zugriff zu gewähren oder abzulehnen, und die Log-Methode zu ändern (siehe Abschnitt 14.2.2).

Folgend ist eine einfaches Beispiel einer Hosts-Zugriffsregel:

```
vsftpd : .example.com
```

Diese Regel leitet TCP Wrappers dazu an, für Verbindungen zum FTP Daemon (`vsftpd`), von jedem Host in der `example.com` Domain, Ausschau zu halten. Sollte diese Regel in `hosts.allow` auftreten, wird die Verbindung angenommen. Sollte diese Regel in `hosts.deny` vorkommen, wird die Verbindung abgelehnt.

Folgendes Beispiel einer Hosts-Zugriffsregel ist komplizierter und verwendet zwei Option-Felder:

```
sshd : .example.com  \
: spawn /bin/echo `/bin/date` access denied>>/var/log/sshd.log \
: deny
```

Beachten Sie, dass in diesem Beispiel jedem der Option-Felder ein Backslash (`\`) voransteht. Die Verwendung eines Backslash beugt einem Ausfallen auf Grund einer zu langen Zeile vor.

Diese Beispielregel sagt, dass wenn ein Verbindungsversuch zum SSH Daemon (`sshd`) von einem Host in der `example.com` Domain stattfindet, führe den Befehl `echo` aus (welcher den Versuch in eine spezielle Log-Datei schreibt), und lehne die Verbindung ab. Da die optionale Anweisung `deny` verwendet wird, wird diese Zeile den Zugriff ablehnen, auch wenn sie in der Datei `hosts.allow` steht. Für einen detaillierteren Überblick der Optionen, sehen Sie Abschnitt 14.2.2.

14.2.1.1. Wildcards

Wildcards erlauben TCP Wrappers eine einfachere Suche von Gruppen von Daemons oder Hosts. Diese werden am häufigsten im Client-Listen-Feld der Zugriffsregel gefunden.

Die folgenden Wildcards können verwendet werden:

- `ALL` — Für Alle. Kann für beide verwendet werden, die Daemon-Liste und die Client-Liste.
- `LOCAL` — Für jeden Host-Rechner, der keinen Punkt (`.`) enthält, wie localhost.
- `KNOWN` — Für jeden Host-Rechner, dessen Hostname und Hostadresse oder der Benutzer bekannt sind.
- `UNKNOWN` — Für jeden Host-Rechner, dessen Hostname und Hostadresse oder der Benutzer nicht bekannt sind.
- `PARANOID` — Für jeden Host-Rechner, dessen Hostname nicht mit der Hostadresse übereinstimmt.

Achtung

Die Wildcards `KNOWN`, `UNKNOWN` und `PARANOID` sollten sehr vorsichtig verwendet werden, da eine Unterbrechung in der Namenauflösung eine Zugriffsverweigerung auf Netzwerkdienste für berechtigte Benutzer zur Folge haben kann.

14.2.1.2. Patterns

Patterns können im Client-Listen-Feld von Zugriffsregeln benutzt werden, um Gruppen von Client-Hosts genauer anzugeben.

Folgend ist eine Liste der am häufigsten akzeptierten Patterns für einen Eintrag in der Client-Liste:

- *Ein mit einem Punkt (.) beginnender Hostname* — Ein Punkt am Anfang eines Hostnamens bewirkt, dass für alle Host-Rechner, die in diesem Hostnamen enden, die Regel angewandt wird. Das folgende Beispiel wird auf jeden Host in der `example.com` Domain angewendet:
  ```
  ALL : .example.com
  ```
- *Eine mit einem Punkt (.) endende IP-Adresse* — Ein Punkt am Ende einer IP-Adresse bewirkt, dass auf alle Hosts, deren IP-Adresse dementsprechend beginnt, die Regel angewendet wird. Das folgende Beispiel trifft auf alle Hosts im `192.168.x.x` Netzwerk zu:
  ```
  ALL : 192.168.
  ```
- *IP Adresse/Netmask Paar* — Netmask-Ausdrücke können auch als ein Pattern verwendet werden, um den Zugriff zu einer bestimmten Gruppe von IP Adressen zu regeln. Das folgende Beispiel trifft auf alle Hosts mit einer Adresse zwischen `192.168.0.0` und `192.168.1.255` zu:
  ```
  ALL : 192.168.0.0/255.255.254.0
  ```

Wichtig

Wenn im IPv4 Adressraum gearbeitet wird, sind Paare von Adresse/Prefixlänge (*prefixlen*) Deklarationen nicht unterstützt. Lediglich IPv6-Regeln können diesed Format benutzen.

- *[IPv6 Adresse]/prefixlen Paar* — [net]/prefixlen Paare können auch als Pattern verwendet werden, um Zugriff zu einer bestimmten Gruppe von IPv6-Adressen zu kontrollieren. Das folgende Beispiel trifft auf jeden Host mit einer Adresse von `3ffe:505:2:1::` bis `3ffe:505:2:1:ffff:ffff:ffff:ffff` zu:
  ```
  ALL : [3ffe:505:2:1::]/64
  ```
- *Ein Stern (*)* — Sterne können für komplette Gruppen von Hostnamen oder IP Adressen verwendet werden, solange diese nicht in einer Client-Liste verwendet werden, welche bereits andere Patterns verwendet. Das folgende Beispiel trifft auf alle Hosts in der `example.com` Domain zu:
  ```
  ALL : *.example.com
  ```
- *Der Slash oder Schrägstrich (/)* — Wenn die Client-Liste mit einem Schrägstrich beginnt, wird diese als Dateiname behandelt. Dies ist nützlich wenn Regeln, welche eine große Anzahl von Hosts angeben, nötig sind. Das folgende Beispiel nimmt Bezug auf TCP Wrappers zur Datei `/etc/telnet.hosts` für alle Telnet-Verbindungen:
  ```
  in.telnetd : /etc/telnet.hosts
  ```

Andere, weniger verwendete Patterns werden auch von TCP Wrappers angenommen. Sehen Sie die man-5-Seite von `hosts_access` für mehr Information.

Warnung

Seien Sie sehr vorsichtig beim Verwenden von Host- und Domain-Namen. Ein Angreifer könnte verschiedene Tricks anwenden, um die richtige Namensauflösung zu umgehen. Zusätzlich verhindert eine Unterbrechung im DNS Service authorisierte Benutzer davon Netzwerk-Services zu verwenden.

Es ist am besten IP Adressen zu verwenden, wenn immer dies möglich ist.

14.2.1.3. Portmap und TCP Wrappers

Verwenden Sie keine Hostnamen, wie `portmap`, beim Erzeugen von Zugriffskontrollregeln für `portmap`, da dessen Implementation von TCP Wrappers Host Look-Ups nicht unterstützt. Aus diesem Grund, verwenden Sie ausschließlich das Schlüsselwort `ALL`, wenn Sie Hosts in `hosts.allow` oder `hosts.deny` angeben.

Außerdem werden Änderungen zu `portmap`-Zugriffskontrollregeln nicht sofort wirksam, ohne dass der `portmap` Service neu gestartet wird.

Da der Betrieb von weit verbreiteten Diensten wie NIS und NFS von `portmap` abhängt, bedenken Sie zuerst diese Einschränkungen.

14.2.1.4. Operatoren

Die Zugriffskontrollregeln kennen zur Zeit einen Operator, `EXCEPT`. Dieser kann sowohl in der Daemon- als auch in der Client-List einer Regel verwendet werden.

Der `EXCEPT` Operator erlaubt spezifische Ausnahmen in einer Regel.

Im folgenden Beispiel der Datei `hosts.allow`, ist es allen `example.com` Hosts erlaubt zu verbinden, mit der Ausnahme von `cracker.example.com`:

```
ALL: .example.com EXCEPT cracker.example.com
```

In einem anderen Beispiel der Datei `hosts.allow`, können Clients des 192.168.0.*x* Netzwerks alle Services benutzen, mit der Ausnahme von FTP:

```
ALL EXCEPT vsftpd: 192.168.0.
```

Anmerkung

Aus organisatorischen Gründen, ist es normalerweise besser `EXCEPT`-Operatoren zu vermeiden. Dadurch können alle Administratoren schnell die gewünschten Dateien durchsuchen, um zu sehen, welche Host-Rechner Zugriff und welche keinen Zugriff auf bestimmte Services haben sollen, ohne mehrere `EXCEPT`-Operatoren durchsuchen zu müssen.

14.2.2. Option-Felder

Zusätzlich zu den grundlegenden Regeln, welche Zugriff gewähren oder ablehnen, unterstützt die Red Hat Enterprise Linux Implementation von TCP Wrappers Erweiterungen zu der Zugriffskontrollsprache durch Optionsfelder. Durch Verwendung der Optionsfelder innerhalb einer Hosts-Zugriffsregel, können Administratoren eine Reihe von Tasks erledigen, wie dem Ändern des Log-Verhaltens, Zusammenfassen der Zugriffskontrolle und dem Ausführen von Shell-Befehlen.

14.2.2.1. Logging

Option-Felder erlauben es Administratoren die Log-Einstellungen und den Schwierigkeitsgrad für eine Regel einfach zu ändern, indem die `severity`-Anweisung verwendet wird.

Im folgenden Beispiel, werden Verbindungen zum SSH Daemon von jedem Host in der `example.com`-Domain zu der Standard-Logdatei `authpriv` geschrieben (da kein Wert angegeben ist), und dies mit einer Priorität von `emerg`:

```
sshd : .example.com : severity emerg
```

Es ist auch möglich, eine Log mit der `severity`-Option anzugeben. Das folgende Beispiel loggt alle Hosts aus der `example.com` Domain, welche versuchen zu einem SSH service zu verbinden, zu der `local0` Log, mit einer Priorität von `alert`:

```
sshd : .example.com : severity local0.alert
```

Anmerkung

In der Praxis, wird dieses Beispiel nicht arbeiten, solange der Syslog-Daemon (`syslogd`) nicht dazu konfiguriert ist, Log-Meldungen zu `local0` zu schreiben. Sehen Sie die `syslog.conf` man-Seite für Informationen zum Konfigurieren von benutzerdefinierten Logs.

14.2.2.2. Zugriffskontrolle

Option-Felder erlauben es dem Administratoren, Hosts explizit anzunehmen oder abzulehnen, indem sie die `allow`- oder `deny`-Anweisung als letzte Option hinzufügen.

Die folgenden Regeln, zum Beispiel, erlauben SSH-Verbindungen von `client-1.example.com`, lehnen aber Verbindungsversuche von `client-2.example.com` ab:

```
sshd : client-1.example.com : allow
sshd : client-2.example.com : deny
```

Durch erlauben der Zugriffskontrolle auf einer pro-Regel Basis, erlaubt das Option-Feld Administratoren alle Zugriffsregeln in entweder `hosts.allow` oder `hosts.deny` zusammenzufassen. Einige halten dies für einen einfacheren Weg die Zugriffsregeln zu organisieren.

14.2.2.3. Shell-Befehle

Option-Felder erlauben Zugriffsregeln Shell-Befehle auszuführen, durch die zwei folgenden Anweisungen:

- `spawn` — Startet einen Shell-Befehl als Kind-Prozess. Diese Option-Anweisung kann Aufgaben wie die Verwendung von `/usr/sbin/safe_finger` durchführen, um weitere Informationen über den anfragenden Client zu erhalten, oder spezielle Log-Dateien mit dem `echo` Befehl erzeugen.

  Im folgenden Beispiel, versuchen Clients auf einen Telnet Service von der `example.com` Domain aus zuzugreifen, was in eine spezielle Log-Datei geschrieben wird:

  ```
  in.telnetd : .example.com \
    : spawn /bin/echo `/bin/date` from %h>>/var/log/telnet.log \
    : allow
  ```

- `twist` — Ersetzt den angeforderten Service mit dem angegebenen Befehl. Diese Anweisung wird oft verwendet, um Fallen für etwaige Angreifer (im Englischen auch "honey pots", Deutsch Honigtöpfe genannt) zu stellen. Diese kann auch verwendet werden um Nachrichten zu verbindenden Clients zu senden. Der twist-Befehl muss am Ende der Regelzeile stehen.

  Im folgenden Beispiel, wird Clients, welche versuchen auf FTP Services von der `example.com` Domain aus zuzugreifen, eine Nachricht mit Hilfe des `echo` Befehls gesendet:

  ```
  vsftpd : .example.com \
  : twist /bin/echo "421 Bad hacker, go away!"
  ```

Für weitere Informationen zur Verwendung von Shell-Befehl Optionen, sehen Sie die `hosts_options` man-Seite.

14.2.2.4. Expansionen

Expansionen, welche im Zusammenhang mit `spawn` und `twist`-Anweisungen verwendet werden, liefern Informationen über den Client, Server und die betreffenden Prozesse.

Folgend ist eine Liste der verfügbaren Expansionen:

- `%a` — Die IP-Adresse des Clients.
- `%A` — Die IP-Adresse des Servers.
- `%c` — Verschiedene Client-Informationen, wie zum Beispiel der Benutzer- und Hostname oder der Benutzername und die IP-Adresse.
- `%d` — Der Name des Daemon-Prozesses.
- `%h` — Der Hostname des Clients (oder IP-Adresse, wenn der Hostname nicht verfügbar ist).
- `%H` — Der Hostname des Servers (oder IP-Adresse, wenn der Hostname nicht verfügbar ist).
- `%n` — Der Hostname des Clients. Wenn dieser nicht verfügbar ist, wird `unknown` ausgegeben. Wenn der Hostname und die Hostadresse des Clients nicht übereinstimmen, `paranoid` ausgegeben.
- `%N` — Der Hostname des Servers. Wenn dieser nicht verfügbar ist, wird `unknown` ausgegeben. Wenn der Hostname und die Hostadresse des Servers nicht übereinstimmen, `paranoid` ausgegeben.
- `%p` — Die ID des Daemonprozesses.
- `%s` — Verschiedene Serverinformationen, wie zum Beispiel der Daemonprozess und die Host- oder IP-Adresse des Servers.
- `%u` — Der Benutzername des Clients. Wenn dieser nicht verfügbar ist, wird `unknown` ausgegeben.

Die folgende Beispielregel verwendet eine Expansion in Verbindung mit dem `spawn` Befehl, um den Host des Clients in einer benutzerdefinierten Log-Datei zu identifizieren.

Sollte ein Verbindungsversuch zum SSH Daemon (`sshd`) von einem Host in der `example.com` Domain unternommen werden, führe den Befehl `echo` aus, um den Versuch in eine spezielle Logdatei zu schreiben, einschließlich desHostnamen des Client (unter Verwendung von `%h`):

```
sshd : .example.com  \
: spawn /bin/echo `/bin/date` access denied to %h>>/var/log/sshd.log \
: deny
```

Ähnlich, können Expansionen dazu verwendet werden, um Nachrichten auf bestimmte Clients abzustimmen. Im folgenden Beispiel, wird Clients, welche versuchen auf FTP Services von der `example.com` Domain aus zuzugreifen, mitgeteilt, dass diese vom Server ausgeschlossen wurden:

```
vsftpd : .example.com \
: twist /bin/echo "421 %h has been banned from this server!"
```

Für eine vollständige Erklärung der verfügbaren Expansionen, wie zusätzlichen Zugriffskontroll-Optionen, sehen Sie Abschnitt 5 der man-Seiten von `hosts_access` (`man 5 hosts_access`) und die man-Seite für `hosts_options`.

Für zusätzliche Informationen zu TCP-Wrappers, sehen Sie Abschnitt 14.5. Für weitere Information zur Sicherung von TCP-Wrappers, sehen Sie das Kapitel *Server-Sicherheit* im *Red Hat Enterprise Linux Sicherheitshandbuch*.

14.3. xinetd

Der xinetd-Daemon ist ein TCP-wrapped *Super Service*, der den Zugriff auf eine Anzahl beliebter Netzwerkservices wie FTP, IMAP und Telnet bereitstellt. Er bietet außerdem servicespezifische Konfigurationsoptionen zur Zugriffskontrolle, erweitertes Logging, Umleitungen und Ressourcen-Einsatzkontrolle.

Wenn sich ein Client Host mit einem von xinetd überwachten Netzwerkservice zu verbinden versucht, erhält der Super Service die Anfrage und prüft die TCP-Wrappers Zugriffsrechte. Wird der Zugang gewährt, überprüft xinetd, dass die Verbindung auch entsprechend seinen Regeln für diesen Service erlaubt ist, und dass der Service nicht mehr als die zugewiesenen Ressourcen verbraucht bzw. jegliche Regeln einhält. Daraufhin wird eine Instanz des angeforderten Services geöffnet und die Überwachung der Verbindung übergeben. Sobald die Verbindung besteht, hält sich xinetd aus der Kommunikation zwischen Client Host und Server raus.

14.4. xinetd-Konfigurationsdateien

Die Konfigurationsdateien für xinetd sind folgende:

- /etc/xinetd.conf — Die globale xinetd Konfigurationsdatei.
- /etc/xinetd.d/ Verzeichnis — Das Verzeichnis, das alle servicespezifischen Dateien enthält.

14.4.1. Die /etc/xinetd.conf Datei

Die Datei /etc/xinetd.conf enthält allgemeine Konfigurationseinstellungen, die jeden Service unter Kontrolle von xinetd betreffen. Bei jedem Start des xinetd Service wird diese Datei gelesen, um also Konfigurationsänderungen wirksam werden zu lassen, muss der Administrator den xinetd Service neu starten. Unten ein Beispiel einer /etc/xinetd.conf Datei:

```
defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
        cps                     = 25 30
}
includedir /etc/xinetd.d
```

Diese Zeilen kontrollieren verschiedene Aspekte von xinetd:

- instances — Bestimmt die Höchstzahl der Anfragen, die xinetd gleichzeitig bearbeiten kann.
- log_type — Weist xinetd an die Protokolldatei authpriv, die Log-Einträge in die Datei /var/log/secure schreibt, zu verwenden. Das Hinzufügen einer Direktive wie FILE /var/log/xinetdlog würde eine benutzerdefinierte Log-Datei mit dem Namen xinetdlog im Verzeichnis /var/log/ erstellen.
- log_on_success — Konfiguriert xinetd zum Protokollieren, wenn die Verbindung erfolgreich ist. Standardmäßig werden die Remote-Host-IP-Adresse und die ID des Servers, der die Anfrage verarbeitet, aufgezeichnet.
- log_on_failure — Konfiguriert xinetd zum Protokollieren wenn die Verbindung fehlschlägt oder nicht zugelassen ist.
- cps — Konfiguriert xinetd, für einen bestimmten Dienst nicht mehr als 25 Verbindungen pro Sekunde zuzulassen. Wenn diese Grenze erreicht wird, wird der Dienst für 30 Sekunden zurückgezogen.

- includedir /etc/xinetd.d/ — Enthält Optionen der servicespezifischen Konfigurationsdateien im Verzeichnis /etc/xinetd.d/. Weitere Informationen zu diesem Verzeichnis finden Sie unter Abschnitt 14.4.2.

Anmerkung

Die Einstellungen log_on_success und log_on_failure in /etc/xinetd.conf werden oftmals von den servicespezifischen Logdateien geändert. Aus diesem Grund können mehr Informationen als von der Datei angezeigt im Servicelog enthalten sein. Weitere Informationen zu Protokoll-Optionen finden Sie unter Abschnitt 14.4.3.1.

14.4.2. Das /etc/xinetd.d/ Verzeichnis

Die Dateien im Verzeichnis /etc/xinetd.d/ enthalten die Konfigurationsdateien für jeden Service, der von xinetd verwaltet wird, sowie die Dateinamen, die zu dem Service gehören. Wie xinetd.conf wird diese Datei nur gelesen, wenn der xinetd Service gestartet wird. Um Änderungen wirksam werden zu lassen, muss der Administrator den xinetd Service neu starten.

Die Dateien in /etc/xinetd.d/ verwenden dieselben Konventionen und Optionen wie /etc/xinetd.conf. Der Hauptgrund dafür, dass sich diese in eigenen Konfigurationsdateien befinden, ist die Anpassung zu vereinfachen und andere Services damit weniger zu beeinflussen.

Um einen Überblick über die Struktur dieser Dateien zu erhalten, betrachten Sie die Datei /etc/xinetd.d/telnet:

```
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = yes
}
```

Diese Zeilen kontrollieren verschiedene Aspekte des vsftpd Service:

- service — Definiert den Servicenamen, meistens entsprechend eines Services in der Datei /etc/services.
- socket_type — Setzt den Netzwerk-Sockettyp auf stream.
- wait — Bestimmt, ob ein Service Single-Threaded (yes) oder Multi-Threaded (no) ist.
- user — Bestimmt die User ID, unter der der Prozess abläuft.
- server — Bestimmt die auszuführende Binärdatei.
- log_on_success — Bestimmt die Protokoll-Parameter für log_on_success zusätzlich zu den in xinetd.conf eingestellten.
- log_on_failure — Bestimmt die Protokoll-Parameter für log_on_failure zusätzlich zu den in xinetd.conf eingestellten.
- disable — Bestimmt, ob der Service aktiv oder inaktiv ist.

14.4.3. Ändern von xinetd Konfigurationsdateien

Es gibt eine große Anzahl an Direktiven für xinetd geschützte Dienste. Dieser Abschnitt beschreibt einige der häufig verwendeten Optionen.

14.4.3.1. Protokoll-Optionen

Die folgenden Protokoll-Optionen stehen für /etc/xinetd.conf und die servicespezifischen Konfigurationsdateien im Verzeichnis /etc/xinetd.d/ zur Verfügung.

Hier eine Liste der häufig verwendeten Protokoll-Optionen:

- ATTEMPT — Protokolliert einen fehlgeschlagenen Versuch (log_on_failure).
- DURATION — Protokolliert die Zeitdauer der Dienstnutzung seitens eines Remote-Systems (log_on_success).
- EXIT — protokolliert das Beenden oder das Endsignal des Dienstes (log_on_success).
- HOST — Protokolliert die IP-Adresse des Remote-Host-Rechners (log_on_failure und log_on_success).
- PID — Protokolliert die Prozess-ID des Servers, an den die Anfrage gesendet wird (log_on_success).
- USERID — Protokolliert den Remote- Benutzer mithilfe der in RFC 1413 definierten Methode für alle Multithreaded-Stream-Dienste (log_on_failure und log_on_success).

Eine vollständige Liste der Protokoll-Optionen finden Sie auf der man-Seite zu xinetd.conf.

14.4.3.2. Zugriffskontroll-Optionen

Benutzer von xinetd-Services können wählen, ob sie die Host-Zugriffskontrolldateien der TCP-Wrappers, Zugriffskontrolle mittels xinetd-Konfigurationsdateien oder eine Mischung von beidem verwenden wollen. Informationen zum Gebrauch von Host-Zugriffskontrolldateien der TCP-Wrappers finden Sie in Abschnitt 14.2.

In diesem Abschnitt wird der Einsatz von xinetd für die Kontrolle von Zugriffen auf bestimmte Services besprochen.

Anmerkung

Im Gegensatz zu TCP-Wrapper, muss der xinetd-Administrator nach jeder Änderung den xinetdService neu starten, damit diese wirksam werden.

Im Gegensatz zu TCP-Wrappers, betrifft die Zugriffskontrolle durch xinetd lediglich die Services, die durch xinetd kontrolliert werden.

Die xinetd-Host-Zugriffskontrolle unterscheidet sich von der von TCP-Wrappers verwendeten Methode. Während TCP-Wrapper die gesamte Zugriffskonfiguration in zwei Dateien ablegt, /etc/hosts.allow und /etc/hosts.deny, kann jede Dienstdatei in /etc/xinetd.d ihre eigenen Zugriffskontrollregeln enthalten.

Die folgenden Optionen werden in den xinetd-Dateien für die Host-Zugriffskontrolle unterstützt:

- only_from — Erlaubt nur den angegebenen Host-Rechnern die Nutzung des Dienstes.
- no_access — Sperrt aufgeführten Host-Rechnern den Zugriff auf den Dienst.

- access_times — Den Zeitraum, in dem ein bestimmter Dienst verwendet werden kann. Der Zeitraum muss im 24-Stunden Format (HH:MM-HH:MM) angegeben werden.

Die Optionen only_from und no_access können eine Liste von IP-Adressen oder Hostnamen verwenden, oder ein gesamtes Netzwerk spezifizieren. Wie TCP-Wrappers, kann durch die Kombination der xinetd-Zugriffskontrolle und der entsprechenden Protokollierkonfiguration die Sicherheit durch das Sperren von Anfragen von gesperrten Hosts und das Protokollieren aller Verbindungsversuche erhöht werden.

Zum Beispiel kann die folgende /etc/xinetd.d/telnet-Datei verwendet werden, um den Telnet-Zugriff einer bestimmten Netzwerkgruppe auf ein System zu verweigern und den gesamten Zeitraum für die Anmeldung von zugelassenen Benutzern einzuschränken:

```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        no_access       = 10.0.1.0/24
        log_on_success  += PID HOST EXIT
        access_times    = 09:45-16:15
}
```

In diesem Beispiel erhält jedes System des Unternetzes 10.0.1.0/24, wie zum Beispiel 10.0.1.2, beim Versuch, auf Telnet zuzugreifen, die folgende Meldung:

```
Connection closed by foreign host.
```

Außerdem werden diese Anmeldeversuche in /var/log/secure protokolliert:

```
May 15 17:38:49 boo xinetd[16252]: START: telnet pid=16256 from=10.0.1.2
May 15 17:38:49 boo xinetd[16256]: FAIL: telnet address from=10.0.1.2
May 15 17:38:49 boo xinetd[16252]: EXIT: telnet status=0 pid=16256
```

Wenn Sie TCP-Wrapper zusammen mit der Zugriffskontrolle von xinetd verwenden, müssen Sie die Beziehung dieser beiden Zugriffskontroll-Mechanismen verstehen.

Im Folgenden wird die Abfolge der Vorgänge in xinetd beschrieben, wenn ein Client eine Verbindung anfordert:

1. Der xinetd-Daemon greift auf die Host-Zugriffsregeln der TCP-Wrapper durch einen libwrap.a Library-Aufruf zu. Besteht eine Dienstverweigerungs-Regel für den Client Host, wird die Verbindung nicht aufgebaut. Besteht eine Zugrifferlaubnis, wird die Verbindung an xinetd weitergegeben.
2. Der xinetd-Daemon überprüft seine eigenen Zugriffskontroll-Regeln für den xinetd-Service und den angeforderten Service. Besteht eine Dienstverweigerungs-Regel für den Client Host, wird die Verbindung nicht aufgebaut. Ansonsten startet xinetd eine Instanz des angeforderten Services und gibt die Kontrolle an diesen weiter.

Wichtig

Seien Sie vorsichtig beim Verwenden von TCP-Wrapper Zugriffskontrollen zusammen mit `xinetd` Zugriffskontrollen. Eine Fehlkonfiguration kann höchst unerwünschte Folgen nach sich ziehen.

14.4.3.3. Bindungs- und Umleitungs-Optionen

Die Dienstkonfigurationsdateien für `xinetd` unterstützen auch die Bindung des Dienstes an eine besondere IP-Adresse und Umleitung der eingehenden Anfragen für diesen Dienst an andere IP-Adressen, Hostnamen oder Ports.

Die Bindung wird von der `bind` -Option in den Dienstkonfigurationsdateien kontrolliert und verknüpft den Dienst mit einer IP-Adresse auf dem System. Nach der Konfiguration lässt die `bind` Option nur Anfragen für die richtige IP-Adresse zum Zugriff auf den Dienst zu. So kann jeder Dienst je nach Bedarf mit verschiedenen Netzwerkschnittstellen gebunden werden.

Dies ist besonders nützlich bei Systemen mit mehreren Netzwerkadaptern oder mehreren IP-Adressen. Sie können beispielsweise Telnet zum Abhören von Schnittstellen konfigurieren, die mit einem privaten Netzwerk und nicht mit dem Internet verbunden sind.

Die Option `redirect` akzeptiert eine IP-Adresse oder einen Hostnamen gefolgt von einer Port-Nummer. Sie konfiguriert den Service, alle alle Anfragen für diesen Dienst an eine bestimmte Adresse und Portnummer weiterzuleiten. Diese Eigenschaft kann verwendet werden, um auf eine andere Port-Nummer auf demselben System zu verweisen, die Anfrage an eine andere IP-Adresse auf demselben Rechner weiterzuleiten, die Anfrage an ein anderes System oder eine andere Port-Nummer zu verschieben. Die Eigenschaft kann auch für eine Kombination dieser Optionen verwendet werden. Auf diese Weise kann ein Benutzer, der sich für einen bestimmten Dienst an einem System anmeldet, ohne Unterbrechung umgeleitet werden.

Der `xinetd`-Daemon kann diese Umleitung durch Erzeugen eines Prozesses ausführen, der während der Verbindung des anfragenden Client-Rechners mit dem Host-Rechner, der den eigentlichen Dienst liefert, im Stay-Alive-Modus läuft, und Daten zwischen den zwei Systemen austauscht.

Der eigentliche Stärke der `bind` und `redirect` -Optionen liegt in deren kombinierten Verwendung. Durch Bindung eines Dienstes an eine bestimmte IP-Adresse auf einem System und dem darauffolgenden Umleiten der Anfragen für denselben Dienst an einen zweiten Rechner, der nur für den ersten Rechner sichtbar ist, können Sie ein internes System verwenden, um Dienste für vollkommen unterschiedliche Netzwerke zur Verfügung zu stellen. Ansonsten können diese Optionen verwendet werden, um die Zeit zu begrenzen, während derer ein Dienst auf einem Multihomed-Rechner einer bekannten IP-Adresse ausgesetzt ist, sowie jegliche Anfragen für diesen Dienst an einen anderen Rechner weiterzuleiten, der eigens für diesen Zweck konfiguriert ist.

Nehmen wir zum Beispiel ein System, das als Firewall mit diesen Einstellungen für seine Telnet-Dienste verwendet wird:

```
service telnet
{
        socket_type  = stream
        wait   = no
        server   = /usr/sbin/in.telnetd
        log_on_success  += DURATION USERID
        log_on_failure  += USERID
        bind                    = 123.123.123.123
        redirect                = 10.0.1.13 23
}
```

Die Optionen `bind` und `redirect` in dieser Datei stellen sicher, dass der telnet-Dienst auf dem Rechner für eine externe IP-Adresse (123.123.123.123) bestimmt ist, und zwar die Internet-seitige. Außer-

dem werden alle an 123.123.123.123 gesendete Telnet-Anfragen über einen zweiten Netzwerkadapter an eine interne IP-Adresse (10.0.1.13) weitergeleitet, auf die nur die Firewall und interne Systeme Zugriff haben. Die Firewall sendet dann die Kommunikation von einem System an das andere, und für das sich verbindende System sieht es so aus, als ob es mit 123.123.123.123 verbunden sei, während es in Wirklichkeit mit einem anderen Rechner verbunden ist.

Diese Eigenschaft ist besonders nützlich für Benutzer mit Breitbandverbindungen und nur für feste IP-Adressen. Wird Network Address Translation (NAT) verwendet, sind die Systems hinter dem Gateway-Rechner, die nur interne IP-Adressen verwenden, außerhalb des Gateway-Systems nicht zugängig. Wenn jedoch bestimmte Services, die mit `xinetd` kontrolliert werden, mit den Optionen `bind` und `redirect` konfiguriert sind, kann der Gateway-Rechner als eine Art Proxy zwischen externen Systemen und einem bestimmten internen Rechner fungieren, der konfiguriert ist, um den Service zur Verfügung zu stellen. Außerdem sind die verschiedenen `xinetd`-Zugriffskontroll- und Protokollieroptionen auch für zusätzlichen Schutz, wie zum Beispiel Begrenzung der Anzahl von gleichzeitigen Verbindungen für den weitergeleiteten Service, verfügbar.

14.4.3.4. Ressourcen-Management-Optionen

Der `xinetd`-Daemon kann einen einfachen Grad an Schutz vor Denial of Service (DoS) Angriffen (Dienstverweigerungs-Angriffe) liefern. Untenstehend finden Sie eine Liste an Direktiven, die Ihnen beim Einschränken der Auswirkung dieser Angriffe helfen:

- `per_source` — Definiert die Höchstanzahl von Verbindungen von einer bestimmen IP-Adresse mit einem bestimmen Dienst. Es werden nur ganze Zahlen als Argument akzeptiert und er kann in `xinetd.conf` und in den servicespezifischen Konfigurationsdateien im Verzeichnis `xinetd.d/` verwendet werden.
- `cps` — Definiert die Höchstzahl der Verbindungen pro Sekunde. Diese Option akzeptiert zwei ganzzahlige Argumente getrennt durch eine Leerstelle. Die erste Zahl ist die Höchstzahl von Verbindungen zum Service pro Sekunde. Die zweite Zahl ist die Anzahl der Sekunden, die `xinetd` warten muss, bis der Service wieder aktiviert wird. Es werden nur ganze Zahlen akzeptiert, und die Option kann in `xinetd.conf` und in den servicespezifischen Konfigurationsdateien im Verzeichnis `xinetd.d/` verwendet werden.
- `max_load` — Definiert den Schwellenwert für die CPU-Nutzung eines Dienstes. Es werden Kommazahlen-Argumente.

Es gibt noch weitere Ressource-Management-Optionen für `xinetd`. Im Kapitel *Server-Sicherheit* im *Red Hat Enterprise Linux Sicherheitshandbuch* und auf der `xinetd.conf` man-Seite finden Sie weitere Informationen.

14.5. Zusätzliche Ressourcen

Weitere Informationen über TCP-Wrappers und `xinetd` finden Sie in der Systemdokumentation und im Internet.

14.5.1. Installierte Dokumentation

Die im Paket enthaltene Dokumentation auf Ihrem System ist ein guter Ausgangspunkt, wenn Sie weitere Informationen über TCP-Wrapper, `xinetd` und Zugriffskontroll-Konfigurationsoptionen suchen.

- /usr/share/doc/tcp_wrappers-<*version*>/ — Enthält eine README-Datei, in der die Funktionsweise von TCP-Wrapper und die verschiedenen Hostnamen- und Hostadressen-Spoofing-Risiken beschrieben werden.
- /usr/share/doc/xinetd-<*version*>/ — Enthält eine README-Datei, in der Aspekte der Zugriffskontrolle beschrieben sind und eine sample.conf-Datei mit Ideen zum Bearbeiten der Konfigurationsdateien im /etc/xinetd.d/ Verzeichnis.
- TCP-Wrappers and xinetd-bezogene man-Seiten — Es gibt eine Reihe von man-Seiten für die verschiedensten Applikationen und Konfigurationsdateien, die im Bezug zu TCP-Wrappers und xinetd stehen. Die folgende Liste benennt einige der wichtigeren man-Seiten.

  Server-Applikationen

  - man xinetd — Die man-Seite für den xinetd Super Service Daemon.

  Konfigurationsdateien

  - man 5 hosts_access — Die man-Seite für die TCP-Wrapper-Hostzugriffskontroll-Dateien.
  - man hosts_options — Die man-Seite für die TCP-Wrapper Optionsfelder.
  - man xinetd.conf — Die man-Seite mit einer Liste der xinetd Konfigurationsoptionen.

14.5.2. Hilfreiche Websites

- http://www.xinetd.org — Die Homepage von xinetd enthält Beispielkonfigurationsdateien, eine vollständige Liste von Eigenschaften und eine FAQ-Liste.
- http://www.macsecurity.org/resources/xinetd/tutorial.shtml — Eine ausführliche Anleitung mit Beispielen, in der viele Möglichkeiten beschrieben werden, standardmäßige xinetd-Konfigurationsdateien für bestimmte Sicherheitszwecke anzupassen.

14.5.3. Bücher zum Thema

- *Red Hat Enterprise Linux Sicherheitshandbuch*; Red Hat, Inc. — Bietet einen Überblick über Workstation-, Server- und Netzwerksicherheit mit speziellen Vorschlägen zu TCP-Wrappers und xinetd.
- *Hacking Linux Exposed* von Brian Hatch, James Lee und George Kurtz; Osbourne/McGraw-Hill — Eine exzellente Ressource für Sicherheit und Informationen TCP-Wrapper und xinetd.

Kapitel 15.

iptables

Red Hat Enterprise Linux wird mit erweiterten Tools für die *Paket-Filterung* geliefert — den Prozess zur Kontrolle von Netzwerkpaketen, mit Zugang zu, durch und aus dem Netzwerkstack des Kernels. Die Kernelversionen vor 2.4 konnten Pakete mit `ipchains` manipulieren und verwendeten Regellisten für jedes Paket in jeder Phase des Filterungsprozesses. Die Einführung des 2.4-Kernels hat `iptables` mit sich gebracht (auch *netfilter* genannt), die den `ipchains` ähnlich sind, deren Wirkungsbereich und Kontrollmöglichkeiten bei der Filterung aber erweitern.

In diesem Kapitel werden die Grundlagen der Paketfilterung beschrieben, wobei die Unterschiede zwischen `ipchains` und `iptables` definiert und die verschiedenen, mit den `iptables`-Befehlen zur Verfügung stehenden Optionen erklärt werden. Es wird außerdem gezeigt, wie Filterungsregeln zwischen den Bootvorgängen des Systems erhalten bleiben.

Wenn Sie Anweisungen für das Erstellen von `iptables`-Regeln oder das Einrichten einer Firewall auf der Grundlage dieser Regeln benötigen, finden Sie weitere Informationen unter Abschnitt 15.7.

Warnung

Der standardmäßige Firewall-Mechanismus im 2.4-Kernel ist zwar `iptables`, `iptables` kann aber nicht benutzt werden, wenn die `ipchains` schon laufen. Wenn also beim Booten `ipchains` vorhanden sind, gibt der Kernel eine Fehlermeldung und kann `iptables` nicht starten.

Diese Bootfehler-Meldungen haben keinerlei Auswirkung auf das Funktionieren der `ipchains`.

15.1. Paket-Filterung

Der Linux-Kernel enthält die integrierte Fähigkeit, Pakete zu filtern und ermöglicht einigen von ihnen den Zugang zum System, während anderen dieser verwehrt wird. Der Netzfilter des 2.4-Kernels enthält integrierte *Tabellen* oder *Regellisten*. Dabei handelt es sich um Folgende:

- `filter` — Die Standardtabelle zum Verwalten von Netzwerkpaketen.
- `nat` — Mithilfe dieser Tabelle werden Pakete geändert, die eine neue Verbindung herstellen, wie für *Network Address Translation* (*NAT*) verwendet.
- `mangle` — Diese Tabelle wird für spezielle Arten der Paketänderung verwendet.

Tipp

Zusätzlich zu diesen eingebauten Tabellen, können spezifische Tabellen erstellt und im Verzeichnis `/lib/modules/<kernel-version>/kernel/net/ipv4/netfilter/` gespeichert werden (wobei `<kernel-version>` der Version des Kernel entspricht.

Jede dieser Tabellen verfügt über eine Gruppe integrierter *Chains* (Ketten), die den Aktionen entsprechen, die vom Netzfilter für das Paket durchgeführt werden.

Die für die `filter`-Tabelle integrierten Chains sind folgende:

- *INPUT* — Gilt für über eine Netzwerkschnittstelle empfangene Pakete.

- *OUTPUT* — Gilt für Pakete, die über dieselbe Netzwerkschnittstelle versendet werden, die die Pakete empfing.
- *FORWARD* — Gilt für Pakete, die auf einer Netzwerkschnittstelle empfangen, aber über eine andere versendet werden.

Die für die `nat`-Tabelle integrierten Chains sind folgende:

- *PREROUTING* — Ändert über eine Netzwerkschnittstelle empfangene Pakete beim Empfang.
- *OUTPUT* — Modifiziert lokal-generierte Netzwerk-Pakete, bevor diese gesendet werden.
- *POSTROUTING* — Ändert Pakete vor dem Senden über eine Netzwerkschnittstelle.

Die für die `mangle`-Tabelle integrierten Chains sind folgende:

- *INPUT* — Ändert für den Host bestimmte Netzwerk-Pakete.
- *OUTPUT* — Modifiziert lokal-generierte Netzwerk-Pakete, bevor diese gesendet werden.
- *FORWARD* — Ändert über den Host gesendete Netzwerk-Pakete.
- *PREROUTING* — Ändert über eine Netzwerkschnittstelle empfangene Pakete vor dem Routen.
- *POSTROUTING* — Ändert Pakete vor dem Senden über eine Netzwerkschnittstelle.

Ein Paket kann in allen Tabellen auf mehrere Regeln hin überprüft werden, bevor es am Ende der Chain austritt. Struktur und Zweck dieser Regeln können unterschiedlich sein, sie versuchen jedoch normalerweise ein Paket, das von einer oder an eine IP-Adresse bzw. mehrere IP-Adressen gesendet wurde, zu identifizieren, wenn dieses ein bestimmtes Protokoll und einen bestimmten Netzwerkdienst benutzt.

Unabhängig von ihrem Ziel sind Pakete, sobald sie einer bestimmten Regel einer Tabelle entsprechen, für ein bestimmtes *Ziel* bzw. für eine auf sie anzuwendende Aktion bestimmt. Wenn in der Regel für das Ziel eines entsprechenden Pakets ein `ACCEPT` (AKZEPTIEREN) angegeben ist, überspringt das Paket die restlichen Regelkontrollen und darf somit seinen Weg in Zielrichtung fortsetzen. Wenn aber in einer Regel für das Ziel `DROP` (AUSLASSEN) angegeben ist, wird das Paket "ausgelassen", d.h. das Paket erhält keinen Zugriff auf das System, und es wird nichts an den Host-Rechner zurückgesendet, von dem das Paket stammt. Wenn eine Regel `QUEUE` (WARTESCHLANGE) als Ziel angibt, wird das Paket zum Benutzerplatz geleitet. Wenn in einer Regel für das Ziel `REJECT` (ABLEHNEN) angegeben ist, wird das Paket ausgelassen und als Fehlerpaket wieder zu seinem Ursprungsort zurückgeschickt.

Jede Chain hat eine Default-Policy zu `ACCEPT`, `DROP`, `REJECT`, oder `QUEUE`. Wenn das Paket keiner der Regeln in der Chain entspricht, wird auf dieses Paket die standardmäßige Policy angewandt.

Der Befehl `iptables` ermöglicht Ihnen diese Tabellen zu konfigurieren, und, falls nötig, neue Tabellen zu erzeugen.

15.2. Unterschiede zwischen `iptables` und `ipchains`

Auf den ersten Blick scheinen sich `ipchains` und `iptables` sehr zu ähneln. Beide Methoden verwenden Regel-Chains für die Filterung von Paketen und arbeiten im Linux-Kernel, nicht nur um zu entscheiden, welche Pakete hinein-oder hinausgelassen werden sollen, sondern auch, wie mit diesen Paketen, die bestimmten Regeln entsprechen, verfahren werden soll. `iptables` stellt Ihnen jedoch eine deutlich erweiterbarere Paketfilterung zur Verfügung, da sie dem Administrator mehr Kontrolle gibt, ohne dass das gesamte System hierdurch zu kompliziert wird.

Insbesondere sollten Benutzer, die sich mit `ipchains` gut auskennen, auf folgende wichtige Unterschiede zwischen `ipchains` und `iptables` achten, bevor sie versuchen, `iptables` zu benutzen:

- *Mit `iptables` wird jedes gefilterte Paket nur durch Anwendung der Regeln einer einzigen Chain und nicht mit denen mehrerer Chains verarbeitet.* Beispiel: Ein FORWARD-Paket, das ein System

betritt, würde mit `ipchains` den INPUT-, FORWARD-, und OUTPUT-Chains unterliegen, um sein Ziel zu erreichen. `iptables` hingegen sendet Pakete nur zur INPUT-Chain, wenn diese für das lokale System bestimmt sind, während Pakete nur an die OUTPUT-Chain gesendet werden, wenn das lokale System die Pakete erzeugt hat. Aus diesem Grund müssen Sie sicherstellen, dass sich die Regel für das Abfangen eines bestimmten Pakets in der richtigen Chain befindet, die das Paket auch wirklich behandelt.

- *Das DENY-Ziel wurde auf DROP geändert.* Mit `ipchains` können Pakete, die einer Regel in einer Chain entsprachen, an das DENY-Ziel weitergeleitet werden, welches unbemerkt das Paket ausgelassen hat. Dieses Ziel muss mit `iptables` auf DROP geändert werden, damit derselbe Effekt erzielt wird.
- *Die Reihenfolge ist wichtig, wenn Optionen in eine Chainregel eingefügt werden.* Bisher war mit `ipchains` die Reihenfolge der Optionen bei der Eingabe einer Regel nicht so wichtig. Der `iptables`-Befehl ist ein wenig empfindlicher dafür, an welcher Stelle Optionen eingefügt werden. Sie müssen nun z.B. den Ursprungs- oder Zielport nach dem in einer Chainregel zu verwendenden Protokoll (ICMP, TCP, oder UDP) spezifizieren.
- *Bei der Spezifizierung von Netzwerkschnittstellen, auf die eine bestimmte Regel angewandt werden soll, müssen Sie Eingangsschnittstellen (`-i` option) nur mit INPUT- oder FORWARD-Chains und Ausgangsschnittstellen (`-o` option) nur mit FORWARD- oder OUTPUT-Chains verwenden.* Dies ist notwendig, weil OUTPUT-Chains nicht mehr für Eingangsschnittstellen verwendet werden und INPUT-Chains für Pakete, die durch eine Schnittstelle treten, nicht gesehen werden.

Dies sind auf keinen Fall alle Änderungen, da `iptables` ein von Grund auf neu geschriebener Netzwerkfilter ist. Genauere Einzelheiten finden Sie im *Linux 2.4 Packet Filtering HOWTO* und in den unter Abschnitt 15.7 angegebenen Quellen.

15.3. Mit `iptables`-Befehlen verwendete Optionen

Regeln, die es ermöglichen, dass Pakete vom Kernel gefiltert werden, werden durch Ausführen des `iptables`-Befehls erstellt. Beim Verwenden des `iptables`-Befehls müssen Sie folgende Optionen angeben:

- *Pakettyp* — Diese Option legt fest, welche Art von Paketen der Befehl filtert.
- *Paketquelle oder -ziel* — Diese Option legt fest, welche Pakete vom Befehl auf Grundlage der Paketquelle oder des Paketziels gefiltert werden.
- *Ziel* — Diese Option legt fest, welche Aktion ausgeführt wird, wenn die Pakete die oben genannten Kriterien erfüllen.

Für weitere Informationen zu spezifischen Optionen, welche diese Aspekte eines Pakets betreffen, sehen Sie Abschnitt 15.3.4 und Abschnitt 15.3.5.

Die mit der gegebenen `iptables`-Regel verwendeten Optionen müssen logisch gruppiert sein, d.h., auf Grundlage des Zwecks und der Bedingungen der Gesamtregel, damit die Regel gültig ist. Der Rest dieses Abschnitts erklärt häufig verwendete Optionen des Befehls `iptables`.

15.3.1. Struktur der `iptables`-Optionen

Viele `iptables`-Befehle haben folgende Struktur:

```
iptables [-t <table-name>] <command> <chain-name> <parameter-1> \
         <option-1> <parameter-n> <option-n>
```

Die Option *<table-name>* erlaubt dem Benutzer eine andere Tabelle als die standardmäßige `filter`-Tabelle auszuwählen, die mit dem Befehl verwendet werden soll. Die Option *<command>* löst einen bestimmten Vorgang aus, wie z.B. das Anhängen oder Löschen einer Regel in einer Chain,

die in der Option <*chain-name*> spezifiziert ist. Nach der Option <*chain-name*> befinden sich Parameterpaare und Optionen, die letztendlich darüber entscheiden, wie die Regel angewandt wird und was passiert, wenn ein Paket einer Regel entspricht.

Bei der Betrachtung der Struktur eines `iptables`-Befehls ist es wichtig, daran zu denken, dass sich anders als bei den meisten anderen Befehlen Länge und Komplexität eines `iptables`-Befehls je nach seinem Zweck verändern können. Ein einfacher Befehl für das Entfernen einer Regel aus einer Chain kann z.B. sehr kurz sein, während ein Befehl für das Filtern von Paketen aus einem bestimmten Sub-Netz aufgrund verschiedener spezifischer Parameter und Optionen sehr lang sein kann. Bei `iptables`-Befehlen sollten Sie berücksichtigen, dass manche Parameter und Optionen, die verwendet werden, unter Umständen die Notwendigkeit nach sich ziehen, weitere Parameter und Optionen zu erstellen, damit die Anforderungen der ersten Option weiter spezifiziert werden können. Um eine gültige Regel zu erstellen, muss diese weitergeführt werden, bis jeder Parameter und jede Option, die einen weiteren Optionensatz erfordert, erfüllt ist.

Wenn Sie `iptables -h` eingeben, erhalten Sie eine vollständige Liste der `iptables`-Befehlsstrukturen.

15.3.2. Befehlsoptionen

Mit Befehlsoptionen wird `iptables` angewiesen, einen bestimmten Vorgang auszuführen. Nur ein einziger Befehl pro `iptables`-Befehlszeichenkette ist zugelassen. Mit Ausnahme des Hilfebefehls sind alle Befehle in Großbuchstaben geschrieben.

Die `iptables`-Befehle sind:

- `-A` — Hängt die `iptables`-Regel an das Ende der spezifizierten Chain an. Dies ist der Befehl, mit dem eine Regel einfach hinzugefügt wird, wenn die Reihenfolge der Regeln in der Chain nicht ausschlaggebend ist.
- `-C` — Kontrolliert eine bestimmte Regel, bevor sie zur benutzerdefinierten Chain hinzugefügt wird. Dieser Befehl kann Ihnen dabei helfen, komplizierte `iptables`-Regeln zu erstellen, indem er Sie jeweils durch Aufforderungen dazu bringt, zusätzliche Parameter und Optionen einzugeben.
- `-D` — Entfernt eine Regel in einer bestimmten Chain nach ihrer Ziffer (z.B. `5` für die 5. Regel einer Chain). Sie können ebenfalls die gesamte Regel eingeben, woraufhin `iptables` dann die entsprechende Regel aus der Chain, mit der die Regel übereinstimmt, entfernt.
- `-E` — Benennt eine benutzerdefinierte Chain um. Dies hat allerdings keine Auswirkung auf die Tabellenstruktur.
- `-F` — Löscht die gewählte Chain, woraufhin effektiv jede Regel in der Chain entfernt wird. Wenn keine Chain angegeben wird, löscht dieser Befehl jede Regel jeder Chain.
- `-h` — Liefert eine Liste mit Befehlsstrukturen sowie eine kurze Zusammenfassung der Befehlsparameter und -Optionen.
- `-I` — Fügt eine Regel an einem bestimmten Punkt in eine Chain ein, welcher ein ganzzahliger Wert ist. Wenn kein Wert angegeben ist, setzt `iptables` den Befehl an den Anfang der Regelliste.

  Achtung

  Achten Sie darauf, dass, wenn Sie die Option `-A` oder `-I` verwenden, die Reihenfolge der Regeln sehr wichtig sein kann, wenn Sie bestimmen, welche Regeln auf welche Pakete zutreffen.

- `-L` — Listet alle Regeln in der nach dem Befehl spezifizierten Chain auf. Um alle Regeln in allen Chains in der Standardtabelle `filter` aufzulisten, spezifizieren Sie nicht eine Chain oder eine Tabelle. Ansonsten sollte folgende Satzstruktur verwendet werden, um die Regeln in einer spezifischen Chain in einer bestimmten Tabelle aufzulisten:
  `iptables -L <chain-name> -t <table-name>`

Zusätzliche Optionen für die `-L`-Befehlsoption, die Regelziffern liefern und ausführlichere Regelbeschreibungen ermöglichen, sind unter anderem in Abschnitt 15.3.6 beschrieben.

- `-N` — Erstellt eine neue Chain mit benutzerdefiniertem Namen.
- `-P` — Setzt die standardmäßige Policy für eine bestimmte Chain, damit bei der Durchquerung von Paketen durch eine Chain, die Pakete, wie bei ACCEPT oder DROP, ohne Übereinstimmung mit einer Regel an ein bestimmtes Ziel weitergeleitet werden können.
- `-R` — Ersetzt eine Regel in einer bestimmten Chain. Sie müssen eine Regelnummer nach dem Namen der Chain verwenden, um die Regel zu ersetzen. Die erste Regel einer Chain bezieht sich auf die Regelziffer eins.
- `-X` — Entfernt eine benutzerdefinierte Chain. Das Entfernen einer integrierten Chain für eine Tabelle ist nicht zugelassen.
- `-Z` — Stellt Byte- und Paketzähler in allen Chains für eine bestimmte Tabelle auf Null.

15.3.3. `iptables` Parameteroptionen

Sobald gewisse `iptables`-Befehle spezifiziert worden sind, einschließlich derer zum Hinzufügen, Anhängen, Entfernen, Einfügen oder Ersetzen innerhalb einer bestimmten Chain, müssen Sie Parameter definieren, um mit der Erstellung einer Paketfilterungsregel beginnen zu können.

- `-c` — Setzt die Zähler für eine bestimmte Regel zurück. Dieser Parameter akzeptiert die `PKTS`- und `BYTES`-Optionen zur Spezifizierung der zurückzusetzenden Zähler.
- `-d` — Stellt Ziel-Hostnamen, IP-Adresse oder Netzwerk eines Pakets ein, das mit der Regel übereinstimmt. Wenn das Paket mit einem Netzwerk übereinstimmt, sind die folgenden Formate für IP-Adressen/Netmasks unterstützt:
  - *`N.N.N.N/M.M.M.M`* — Wobei *`N.N.N.N`* der Bereich der IP-Adresse und *`M.M.M.M`* die Netmask ist.
  - *`N.N.N.N/M`* — Wobei *`N.N.N.N`* der Bereich der IP-Adresse und *`M`* die Bitmask ist.
- `-f` — Wendet diese Regel nur auf fragmentierte Pakete an.

  Durch Verwendung der `!`-Option nach diesem Parameter werden nur unfragmentierte Parameter abgefangen.
- `-i` — Setzt die Schnittstelle des Eingangsnetzwerks, z.B. `eth0` oder `ppp0`, die für eine bestimmte Regel benutzt werden soll. Mit `iptables` sollte dieser zusätzliche Parameter nur mit INPUT- und FORWARD-Chains in Verbindung mit der `filter`-Tabelle und der PREROUTING-Chain mit den `nat`- und `mangle`-Tabellen verwendet werden.

  Dieser Parameter unterstützt auch folgende spezielle Optionen:
  - `!` — Weist diesen Parameter an, keine entsprechenden Übereinstimmungen zu suchen bzw. jede spezifizierte Schnittstelle von dieser Regel auszuschließen.
  - `+` — Ein Platzhalterzeichen, das verwendet wird, um alle Schnittstellen zu kontrollieren, die einer bestimmten Zeichenkette entsprechen. Der `-i eth+`-Parameter würde diese Regel z.B. für alle Ethnernet-Schnittstellen Ihres Systems anwenden, aber alle anderen Schnittstellen, wie z.B. `ppp0` auslassen.

  Wenn der `-i`-Parameter ohne Spezifizierung einer Schnittstelle verwendet wird, ist jede Schnittstelle von dieser Regel betroffen.
- `-j` — Weist `iptables` an, ein bestimmtes Ziel zu übergehen, wenn ein Paket einer bestimmten Regel entspricht. Gültige Ziele, die nach der `-j`-Option verwendet werden können, sind unter anderem die Standardoptionen `ACCEPT`, `DROP`, `QUEUE` und `RETURN` sowie erweiterte Optionen,

die über Module verfügbar sind, die standardmäßig mit mit dem Red Hat Enterprise Linux `iptables`RPM-Paket geladen werden, wie z.B. unter anderem `LOG`, `MARK` und `REJECT`. Weitere Informationen zu diesen und anderen Zielen sowie Regeln zu deren Verwendung finden Sie auf der `iptables`-man-Seite.

Sie können ein Paket, das dieser Regel entspricht, auch an eine benutzerdefinierte Chain außerhalb der aktuellen Chain weiterleiten. Dadurch können Sie andere Regeln auf dieses Paket anwenden.

Wenn kein Ziel festgelegt ist, bewegt sich das Paket an der Regel vorbei, ohne dass etwas passieren würde. Der Zähler für diese Regel springt jedoch um eine Stelle weiter.

- `-o` — Setzt die Schnittstelle des Ausgangsnetzwerks für eine bestimmte Regel fest, die nur mit OUTPUT- un d FORWARD-Chains in der `filter`-Tabelle und mit der POSTROUTING-Chain in den `nat`- und `mangle`-Tabellen verwendet werden kann. Die Optionen dieses Parameters sind dieselben wie die des Parameters der Schnittstelle des Eingangsnetzwerks (`-i`).
- `-p` — Setzt das IP-Protokoll für die Regel, die entweder `icmp`, `tcp`, `udp` oder `all` sein kann, um allen möglichen Protokollen zu entsprechen. Außerdem können weniger verwendete Protokolle, die in `/etc/protocols` aufgelistet sind, ebenfalls verwendet werden. Wenn diese Option beim Erstellen einer Regel ausgelassen wird, ist die `all`-Option der Standard.
- `-s` — Setzt die Quelle eines bestimmten Pakets mit Hilfe derselben Satzstrukturen, die der Zielparameter (`-d`) verwendet.

15.3.4. `iptables` Match-Optionen

Verschiedene Netzwerkprotokolle ermöglichen spezielle Übereinstimmungsoptionen, die auf spezifische Weise gesetzt werden können, um ein bestimmtes Paket mit Hilfe dieses Protokolls zu kontrollieren. Das Protokoll muss natürlich zuerst im `iptables`-Befehl spezifiziert werden, z.B. durch die Verwendung von `-p tcp` <*Protokollname*> (wobei <*Protokollname*> das Ziel-Protokoll ist) die Optionen für dieses Protokoll verfügbar zu machen.

15.3.4.1. TCP-Protokoll

Folgende Übereinstimmungsoptionen stehen für das TCP-Protokoll zur Verfügung (`-p tcp`):

- `--dport` — Setzt den Zielport für das Paket. Für die Konfiguration dieser Option können Sie entweder den Namen eines Netzwerkdienstes verwenden (z.B. `www` oder `smtp`) und eine oder mehrere Portnummern verwenden. Um die Namen und Alias-Namen der Netzwerkdienste und die Portnummern, die Sie verwenden, nachzulesen, sehen Sie sich bitte die Datei `/etc/services` an. Sie können auch `--destination-port` verwenden, um diese Übereinstimmungsoption zu spezifizieren.

  Um eine spezifische Reihe von Portnummern anzugeben, trennen Sie die zwei Ziffern durch einen Doppelpunkt (`:`), z.B.: `-p tcp --dport 3000:3200`. Die längstmögliche Reihe ist `0:65535`.

  Sie können auch ein Ausrufezeichen (`!`) als Flag nach der `--dport`-Option verwenden, um `iptables` anzuweisen, alle Pakete, die *nicht* diesen Netzwerkdienst oder diesen Port verwenden, zu kontrollieren.
- `--sport` — Setzt den Ursprungsport des Pakets unter Verwendung der selben Optionen wie `--dport`. Sie können auch `--source-port` verwenden, um diese Übereinstimmungsoption zu spezifizieren.
- `--syn` — Kontrolliert alle TCP-Pakete, die eine Kommunikation initialisieren sollen, allgemein *SYN-Pakete* genannt, auf Übereinstimmung mit dieser Regel. Alle Pakete, die einen Daten-Payload enthalten, werden nicht bearbeitet. Wird ein Ausrufezeichen (`!`) als Flag hinter die `--syn`-Option gesetzt, werden alle Nicht-SYN-Pakete kontrolliert.
- `--tcp-flags` — Ermöglicht die Verwendung von TCP-Paketen mit bestimmten Bits oder Flags, damit sie einer Regel entsprechen. Die Übereinstimmungsoption `--tcp-flags` akzeptiert nach-

stehend zwei Parameter, die Flags für bestimmte Bits in einer Liste mit Kommatrennung sind. Der erste Parameter ist eine Maske, die die zu untersuchenden Flags des Pakets bestimmt. Der zweite Parameter bezieht sich auf die Flags, die im Paket gesetzt werden müssen, um eine Übereinstimmung zu erhalten.

Mögliche Flags sind:

- `ACK`
- `FIN`
- `PSH`
- `RST`
- `SYN`
- `URG`
- `ALL`
- `NONE`

Eine `iptables`-Regel, die `-p tcp --tcp-flags ACK,FIN,SYN SYN` enthält, überprüft beispielsweise nur TCP-Pakete, in denen das SYN-Flag aktiviert und die ACK- und FIN-Flags deaktiviert sind.

Wie bei vielen anderen Optionen auch, wird die Auswirkung der Überprüfungsoptionen durch Einfügen eines Ausrufezeichens (`!`) hinter `--tcp-flags` umgekehrt, so dass für deren Überprüfung die Flags des zweiten Parameters nicht in Reihenfolge gesetzt werden müssen.

- `--tcp-option` — Versucht mit Hilfe von TCP-spezifischen Optionen zu überprüfen, die innerhalb eines bestimmten Pakets aktiviert werden können. Diese Übereinstimmungsoption kann ebenfalls mit dem Ausrufezeichen (`!`) umgekehrt werden.

15.3.4.2. UDP-Protokoll

Für das UDP-Protokoll stehen folgende Übereinstimmungsoptionen zur Verfügung(`-p udp`):

- `--dport` — Spezifiziert den Zielport des UDP-Pakets unter Verwendung von Dienstnamen, Portnummer oder einer Reihe von Portnummern. Die `--destination-port`-Übereinstimmungsoption kann an Stelle von `--dport` benutzt werden. Vgl. hierzu die `--dport`-Übereinstimmungsoption in Abschnitt 15.3.4.1 für die verschiedenen Verwendungsmethoden dieser Option.
- `--sport` — Bestimmt den Ursprungsport des UDP-Pakets unter Verwendung von Dienstnamen, Portnummer oder einer Reihe von Portnummern. Die `--source-port`-Übereinstimmungsfunktion kann an Stelle von `--sport` verwendet werden. Vgl. hierzu die `--dport`- Übereinstimmungsfunktion in Abschnitt 15.3.4.1 für die vielen unterschiedlichen Verwendungsmöglichkeiten dieser Option.

15.3.4.3. ICMP-Protokoll

Diese folgenden Match-Optionen sind für das Internet Control Message Protocol (ICMP) (`-p icmp`) verfügbar:

- `--icmp-type` — Bestimmt den Namen oder die Nummer des ICMP-Typs, der mit der Regel übereinstimmen soll. Durch Eingabe des Befehls `iptables -p icmp -h` wird eine Liste aller gültigen ICMP-Namen angezeigt.

15.3.4.4. Module mit zusätzlichen Match-Optionen

Zusätzliche Übereinstimmungsoptionen, die sich nicht spezifisch auf ein Protokoll beziehen, sind ebenfalls mithilfe von Modulen verfügbar, die geladen werden, wenn der `iptables`- Befehl sie aufruft. Um ein Übereinstimmungsmodul anzuwenden, müssen Sie das Modul mit dessen Namen laden, indem beim Erstellen einer Regel der `-m` *<Modulname>* (wobei *<Modulname>* durch den Namen des Moduls ersetzt wird) in den `iptables`-Befehl eingefügt wird.

Standardmäßig stehen zahlreiche Module zur Verfügung. Sie können auch Ihre eigenen Module erstellen, um die Funktionalität zu erweitern.

Folgend ist eine Teilliste der am häufigsten verwendeten Module:

- `limit`-Modul — Erlaubt eine Grenze für die Anzahl der in Übereinstimmung mit einer Regel zu überprüfenden Pakete zu setzen. Dies ist besonders nützlich, wenn zusammen mit einem `LOG`-Target verwendet. Auf diese Weise verhindern Sie, dass die zahlreichen übereinstimmenden Pakete Ihre Protokolldateien nicht mit wiederholten Nachrichten überfüllen oder zu viele Systemressourcen beanspruchen. Sehen Sie Abschnitt 15.3.5 für weitere Informationen zum `LOG`-Target.

  Das `limit`-Modul erlaubt die folgenden Optionen:

  - `--limit` — Bestimmt die Zahl der Übereinstimmungen innerhalb eines bestimmten Zeitraums, der mit einem Anzahl- und Zeitmodifikator in dem Format *<number>* `/`*<Zeit>* angegeben wird. Mit `--limit 5/hour`, zum Beispiel, kann die Regel nur `5` Mal in einer Stunde übereinstimmen.

    Wenn keine Anzahl- und Zeitarbeiter angegeben sind, wird der Standardwert `3/hour` angenommen.

  - `--limit-burst` — Setzt eine Grenze für die Anzahl von Paketen, deren Übereinstimmung mit einer Regel gleichzeitig geprüft `--limit`-Option verwendet werden. Man kann außerdem einen maximalen Grenzwert setzen.

    Wenn keine Zahl festgelegt wird, können anfangs nur fünf Pakete in Übereinstimmung mit der Regel überprüft werden.

- `state`-Modul — Dieses Modul, welches die `--state`-Übereinstimmungsoptionen definiert, kann ein Paket auf die nachfolgenden, bestimmten Verbindungszustände überprüfen:

  Das Modul `state` erlaubt die folgenden Optionen:

  - `--state` — Übereinstimmung mit einem Paket, das folgenden Verbindungszustände hat:

    - `ESTABLISHED` — Das übereinstimmende Paket wird anderen Paketen in einer bestimmten Verbindung zugeordnet.
    - `INVALID` — Das übereinstimmende Paket kann nicht mit einer bekannten Verbindung verknüpft werden.
    - `NEW` — Das übereinstimmende Paket stellt entweder eine neue Verbindung her oder ist Teil einer Zwei-Weg-Verbindung, die vorher nicht gesehen wurde.
    - `RELATED` — Ein übereinstimmendes Paket stellt eine neue Verbindung her, die auf irgendeine Weise mit einer bestehenden Verbindung zusammenhängt.

    Die Verbindungsstatus können untereinander miteinander verbunden werden, indem sie durch Kommata voneinander getrennt werden, wie z.B. in `-m state --state INVALID,NEW`.

- `mac`-Modul — Dieses Modul ermöglicht die Übereinstimmung einer bestimmten Hardware-MAC-Adresse zu überprüfen.

  Das `mac`-Modul hat folgende Option:

- `--mac-source` — Überprüft auf die MAC-Adresse der NIC, welche das Paket gesendet hat. Um eine MAC-Adresse von einer Regel auszuschließen, fügen Sie nach der `--mac-source`-Übereinstimmungsoption ein Ausrufezeichen (`!`) hinzu.

Weitere, über Module verfügbare Übereinstimmungsoptionen finden Sie auf der man-Seite zu `iptables`.

15.3.5. Zieloptionen

Sobald ein Paket mit einer bestimmten Regel übereinstimmt, kann die Regel das Paket an viele verschiedene Ziele senden, an denen dann eventuell weitere Vorgänge erfolgen. Außerdem hat jede Chain ein standardmäßiges Ziel, das verwendet wird, wenn ein Paket keiner Regel entspricht oder wenn in der Regel, mit dem das Paket übereinstimmt, ein Ziel angegeben ist.

Die Folgenden sind die Standardziele:

- *<user-defined-chain>* — *<user-defined-chain>* steht hier für den Namen der benutzerdefinierten Chain. Dieses Ziel leitet das Paket zur Ziel-Chain weiter.
- `ACCEPT` — Das Paket gelangt erfolgreich an sein Ziel oder an eine andere Chain.
- `DROP` — Das Paket wird "ausgelassen". Das System, das dieses Paket gesendet hat, wird nicht über das "Ausfallen" des Pakets benachrichtigt.
- `QUEUE` — Das Paket wird zur Warteschlange für die Bearbeitung durch eine Benutzerraum-Applikation hinzugefügt.
- `RETURN` — Hält die Überprüfung der Übereinstimmung des Pakets mit Regeln in der aktuellen Chain an. Wenn das Paket mit einem `RETURN`-Ziel mit einer Regel in einer Chain übereinstimmt, die von einer anderen Chain aufgerufen wurde, wird das Paket an die erste Chain zurückgesendet, damit die Überprüfung wieder dort aufgenommen werden kann, wo sie unterbrochen wurde. Wenn die `RETURN`-Regel in einer integrierten Chain verwendet wird und das Paket nicht zu seiner vorherigen Chain zurückkehren kann, entscheidet das Standardziel für die aktuelle Chain, welche Maßnahme getroffen wird.

Zusätzlich zu diesen Standardzielen können auch noch verschiedene andere Ziele mit Erweiterungen verwendet werden, sogenannte *Zielmodule*. Weitere Informationen zu Übereinstimmungsoptionsmodulen finden Sie unter Abschnitt 15.3.4.4.

Es gibt viele erweiterte Zielmodule, von denen sich die meisten auf bestimmte Tabellen oder Situationen beziehen. Einige der bekanntesten Zielmodule, die standardmäßig in Red Hat Enterprise Linux enthalten sind:

- `LOG` — Protokolliert alle Pakete, die dieser Regel entsprechen. Da die Pakete vom Kernel protokolliert werden, bestimmt die `/etc/syslog.conf`-Datei, wo diese Protokolldateien geschrieben werden. Standardmäßig werden sie in der `/var/log/messages`-Datei abgelegt.

  Nach dem `LOG`-Ziel können verschiedene Optionen verwendet werden, um die Art des Protokolls zu bestimmen:

  - `--log-level` — Bestimmt die Prioritätsstufe eines Protokolliervorgangs. Auf den man-Seiten von `syslog.conf`- finden Sie eine Liste der Prioritätsstufen.
  - `--log-ip-options` — Alle in den Kopfzeilen eines IP-Pakets enthaltenen Optionen werden protokolliert.
  - `--log-prefix` — Fügt beim Schreiben einer Protokollzeile eine Zeichenkette vor der Protokollzeile ein. Es werden bis zu 29 Zeichen nach der `--log-prefix`- Option akzeptiert. Dies

ist auch beim Schreiben von syslog-Filtern im Zusammenhang mit der Paketprotokollierung sehr nützlich.

- `--log-tcp-options` — Alle in den Kopfzeilen eines TCP-Pakets enthaltenen Optionen werden protokolliert.
- `--log-tcp-sequence` — Schreibt die TCP- Sequenznummer für das Paket in der Protokolldatei.

- `REJECT` — Sendet ein Fehlerpaket an das System zurück, das das Paket gesendet hat, und lässt dieses dann "aus" (DROP).

  Mit dem `REJECT`-Ziel kann die `--reject-with <Typ>` -Option verwendet werden, um mehrere Details zusammen mit dem Fehlerpaket zu senden. Die Meldung `port-unreachable` ist die standardmäßige <*type*>-Fehlermeldung (wobei <*type*> die Art der Zurückweisung angibt), die angezeigt wird, wenn keine andere Option angewandt wurde. Eine vollständige Liste der verwendbaren <*type*>-Optionen finden Sie auf der `iptables`-man-Seite.

Andere Zielerweiterungen, die für die Maskierung unter Verwendung der `nat`-Tabelle oder für Paketänderung mithilfe der `mangle`-Tabelle nützlich sind, finden Sie auf der `iptables`-man-Seite.

15.3.6. Auflistungsoptionen

Der standardmäßige Auflistungsbefehl `iptables -L` bietet eine sehr allgemeine Übersicht über die standardmäßigen aktuellen Regel-Chains der Filtertabelle. Es gibt aber auch noch zusätzliche Optionen mit weiteren Informationen:

- `-v` — Zeigt eine ausführliche Ausgabe an, wie z.B. die Anzahl der Pakete und Bytes, die jede Chain gesehen hat, die Anzahl der Pakete und Bytes, die von jeder Regel auf Übereinstimmung überprüft wurden und auf deren Schnittstellen eine bestimmte Regel angewandt werden.
- `-x` — Erweitert die Zahlen auf ihre exakten Werte. In einem arbeitenden System kann die Anzahl der Pakte und Bytes, die von einer bestimmten Chain oder Regel gesehen werden, unter Verwendung der Abkürzungen `K` (Tausender), `M` (Millionen) und `G` (Milliarden) am Ende der Zahl wiedergegeben werden. Mit dieser Option muss zwangsläufig die vollständige Zahl angezeigt werden.
- `-n` — Zeigt IP-Adressen und Portnummern im numerischen Format an, und nicht im standardmäßigen Hostnamen- und Netzwerkdienst-Format.
- `--line-numbers` — Listet Regeln in jeder Chain in Nähe derer numerischer Reihenfolge in der Chain auf. Diese Option ist nützlich, wenn man versucht, eine bestimmte Regel aus einer Chain zu entfernen oder zu bestimmen, wo eine Regel in einer Chain eingefügt werden soll.
- `-t` — Gibt einen Tabellennamen an.

15.4. `iptables`-Regeln werden gespeichert

Regeln, die mit dem `iptables`-Befehl erstellt wurden, werden nur im RAM gespeichert. Wenn das System nach Erstellung der `iptables`-Regeln neu gestartet wird, gehen diese verloren. Wenn Sie möchten, dass Netzfilterregeln bei jedem Booten Ihres Systems erneut wirksam werden, müssen Sie sich als root anmelden und folgendes eingeben:

```
/sbin/service iptables save
```

Dadurch wird das iptables-Init-Skript angewiesen, das aktuelle /sbin/iptables-save-Programm auszuführen und die aktuelle iptables-Konfiguration in die /etc/sysconfig/iptables-Datei geschrieben. Die bestehende Datei /etc/sysconfig/iptables wird unter /etc/sysconfig/iptables.save gespeichert.

Beim nächsten Systemstart wendet das iptables-Init-Skript die in /etc/sysconfig/iptables gespeicherten Regeln durch die Verwendung des /sbin/iptables-restore-Befehls erneut an.

Es ist grundsätzlich empfehlenswert, eine neue iptables-Regel immer erst zu testen, bevor sie in die /etc/sysconfig/iptables-Datei eingefügt wird. Sie können die iptables-Regeln aber auch von der Dateiversion eines anderen Systems in diese Datei kopieren, wodurch sie in kurzer Zeit ganze Sätze von iptables-Regeln an verschiedene Rechner verteilen können.

Wichtig

Wenn Sie die /etc/sysconfig/iptables-Datei an andere Rechner verteilen, müssen Sie /sbin/service iptables restart eingeben, damit die neuen Regeln wirksam werden.

15.5. iptables Kontrollskripte

Unter Red Hat Enterprise Linux gibt es zwei grundlegende Methoden iptables zu kontrollieren.

- **Security Level Configuration Tool** (redhat-config-securitylevel) — Eine grafische Benutzeroberfläche zum Erstellen, Aktivieren und Speichern von grundlegenden Firewall-Einstellungen. Für weitere Informationen zur Verwendung dieses Tools, sehen Sie das Kapitel *Grundlegende Firewall-Konfiguration* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.
- /sbin/service iptables <*option*> — Ein vom root-Benutzer ausgeführter Befehl, der iptables, über deren Init-Skripte, aktiviert, deaktiviert oder andere Funktionen ausführt. <*option*> steht hierbei für eine der folgenden Anweisungen:
  - start — Ist eine Firewall konfiguriert (d.h. /etc/sysconfig/iptables ist vorhanden), werden alle laufenden iptables beendet und dann mit dem Befehl /sbin/iptables-restore gestartet. Die start-Anweisung arbeitet nur dann, wenn das ipchains Kernel-Modul nicht geladen ist.
  - stop — Wenn eine Firewall im Einsatz ist, werden die Firewall-Regeln im Speicher gelöscht und alle iptables-Module und Helfer beendet.

    Wenn die IPTABLES_SAVE_ON_STOP-Anweisung in der Konfigurationsdatei /etc/sysconfig/iptables-config vom Standardwert auf yes geändert wird, werden die augenblicklichen Regeln unter /etc/sysconfig/iptables gespeichert und jede bestehende Regel nach /etc/sysconfig/iptables.save verschoben.

    Sehen Sie Abschnitt 15.5.1 für weitere Informationen zur Datei iptables-config.
  - restart — Sollte eine Firewall in Betrieb sein, werden die Firewall-Regeln im Speicher gelöscht und die Firewall, sollte sie in /etc/sysconfig/iptables konfiguriert sein, neu gestartet. Die restart-Anweisung wird nur dann arbeiten, wenn die ipchains Kernel-Module nicht geladen sind.

    Wenn die IPTABLES_SAVE_ON_RESTART-Anweisung der Konfigurationsdatei /etc/sysconfig/iptables-config vom Standardwert auf yes geändert wird, werden die augenblicklichen Regeln unter /etc/sysconfig/iptables gespeichert und jede bestehende Regel nach /etc/sysconfig/iptables.save verschoben.

Sehen Sie Abschnitt 15.5.1 für weitere Informationen zur Datei `iptables-config`.

- `status` — Gibt den Status der Firewall und eine Liste der aktiven Regeln am Shell-Prompt aus. Sollten keine Firewall-Regeln geladen oder konfiguriert sein, wird dies angegeben.

  Eine Liste der aktiven Regeln, die Domain- und Hostnamen in den Regellisten enthalten, solange der Standardwert für `IPTABLES_STATUS_NUMERIC` is in der Konfigurationsdatei `/etc/sysconfig/iptables-config` nicht auf `yes` geändert wird. Sehen Sie Abschnitt 15.5.1 für weitere Informationen zur Datei `iptables-config`.

- `panic` — Löscht alle Firewall-Regeln. Die Policy aller konfigurierten Tabellen wird auf `DROP` gesetzt.

- `save` — Speichert Firewall-Regeln mittels `iptables-save` nach `/etc/sysconfig/iptables`. Sehen Sie Abschnitt 15.4 für weitere Informationen zum Speichern von Firewall-Regeln.

Tipp

Um die gleichen Initskript-Befehle zu verwenden, um den Netfilter für IPv6 zu kontrollieren, ersetzen Sie `iptables` durch `ip6tables` in den in diesem Abschnitt angegebenen `/sbin/service` Befehlen. Für weitere Informationen zu IPv6 und Netfilter, sehen Sie Abschnitt 15.6.

15.5.1. Konfigurationsdatei der `iptables` Kontrollskripte

Das Verhalten des `iptables`-Init-Skripts wird durch die Konfigurationsdatei `/etc/sysconfig/iptables-config` bestimmt. Folgend ist eine Liste der in dieser Datei vorkommenden Anweisungen:

- `IPTABLES_MODULES` — Gibt eine durch Leerzeichen getrennte Liste von zusätzlichen `iptables`-Modulen an, die beim aktivieren einer Firewall geladen wird. Diese kann Verbindungs-Tracker und NAT Helfer enthalten.
- `IPTABLES_SAVE_ON_STOP` — Speichert die augenblicklichen Firewall-Regeln nach `/etc/sysconfig/iptables`, wenn die Firewall angehalten wird. Diese Anweisung akzeptiert folgende Werte:
  - `yes` — Speichert vorhandene Regeln nach `/etc/sysconfig/iptables`, wenn die Firewall angehalten wird. Die vorherige Version wird unter `/etc/sysconfig/iptables.save` abgelegt.
  - `no` — Der Standardwert. Bestehende Regeln werden nicht gespeichert, wenn die Firewall angehalten wird.

- `IPTABLES_SAVE_ON_RESTART` — Speichert augenblickliche Firewall-Regeln wenn die Firewall neu gestartet wird. Diese Anweisungen akzeptiert die folgenden Werte:
  - `yes` — Speichere bestehende Regeln nach `/etc/sysconfig/iptables`, wenn die Firewall neu gestartet wird. Die vorherige Version wird dabei unter `/etc/sysconfig/iptables.save` abgelegt.
  - `no` — Der Standardwert. Bestehende Regeln werden nicht gespeichert, wenn die Firewall neu gestartet wird.

- IPTABLES_SAVE_COUNTER — Speichert und stellt alle Paket- und Byte-Zähler in allen Ketten und Regeln wieder her. Diese Anweisung akzeptiert die folgenden Werte:
  - yes — Speichere die Werte der Zähler.
  - no — Der Standardwert. Speichert die Werte der Zähler nicht.

- IPTABLES_STATUS_NUMERIC — Gibt die IP-Adressen anstelle der Domain- oder Hostnamen in der Statusanzeige aus. Diese Anweisung akzeptiert die folgenden Werte:
  - yes — Gibt lediglich IP-Adressen in der Statusanzeige aus.
  - no — Der Standardwert. Gibt Domain- oder Hostnamen in der Statusanzeige aus.

15.6. ip6tables und IPv6

Sollte das iptables-ipv6 Paket installiert sein, kann Netfilter unter Red Hat Enterprise Linux das IPv6 Internet-Protokoll der nächsten Generation behandeln. Der Befehl zur Manipulation des IPv6 Netfilters ist ip6tables. Die meisten Anweisungen für diesen Befehl sind identisch zu denen von iptables, ausser, dass die nat-Tabelle noch nicht unterstützt ist. Das heisst, dass es noch nicht möglich ist, IPv6 Network-Address-Translation Tasks durchzuführen, wie Masquerading und Port-Forwarding.

Gespeicherte Regeln für ip6tables sind in der Datei /etc/sysconfig/ip6tables. Alte, durch die ip6tables-Initskripte gespeicherte Regeln, sind in der Datei /etc/sysconfig/ip6tables.save.

Die Konfigurationsdatei für ip6tables-Initskripte ist /etc/sysconfig/ip6tables-config und die Namen der Anweisungen sind leicht verschieden. Die iptables-config Anweisung, zum Beispiel, IPTABLES_MODULES ist IP6TABLES_MODULES in ip6tables-config.

15.7. Zusätzliche Informationsquellen

Zusätzliche Informationen zur Paketfilterung mit iptables finden Sie in den weiter unten aufgeführten Quellen.

15.7.1. Installierte Dokumentation

- man iptables — Enthält eine Beschreibung von iptables, und eine umfangreiche Liste verschiedener Befehle, Parameter und anderer Optionen.

15.7.2. Hilfreiche Websites

- http://netfilter.samba.org — Die Homepage des Netfilter/iptables Projektes. Enthält ausgewählte Informationen zu iptables sowie FAQ zu spezifischen Problemen, denen Sie unter Umständen begegnen, verschiedene hilfreiche Handbücher von Rusty Russell, dem Linux-IP-Firewall-Warter. In diesen Anleitungen werden Themen, wie z.B. Netzwerkgundlagen, 2.4-Kernel-Paketfilterung und NAT-Konfigurationen besprochen.

- http://www.linuxnewbie.org/nhf/Security/ IPtables_Basics.html — Ein sehr allgemeiner Überblick darüber, wie sich Pakete durch den Linux-Kernel bewegen, plus eine Einleitung zur Erstellung von einfachen `iptables`-Befehlen.
- http://www.redhat.com/support/resources/networking/firewall.html — Auf dieser Webseite finden Sie die aktuellsten Links zu Informationsquellen zum Thema Paketfilterung.
- *Red Hat Enterprise Linux Sicherheitshandbuch*; Red Hat, Inc. — Enthält ein Kapitel zur Rolle von Firewalls innerhalb einer globalen Sicherheitsstrategie, wie auch Strategien zum Erstellen von Firewall-Regeln.
- *Red Hat Enterprise Linux Handbuch zur System-Administration*; Red Hat, Inc. — Enthält ein Kapitel zur Konfiguration von Firewalls, unter Verwendung von **Security Level Configuration Tool**.

redhat

Kapitel 16.

Kerberos

Systemsicherheit und -Integrität innerhalb eines Netzwerkes kann ziemlich schwierig sein, und die Zeit mehrerer Systemadministratoren allein nur für das Verfolgen von welche Services auf dem Netzwerk ausgeführt und wie diese ausgeführt werden, in Anspruch nehmen. Desweiteren kann das Authentifizieren von Benutzern für Netzwerkservices gewisse Gefahren bergen, wenn die Methoden hierfür von Natur aus unsicher sind, wie am Beispiel von Übertragungen unverschlüsselter Passwörter über ein Netzwerk unter FTP- oder Telnetprotokollen bewiesen. Kerberos ist eine Methode, die Notwendigkeit von Protokollen, die eine unsichere Authentifizierung ermöglichen, auszuräumen und somit die Gesamtsicherheit des Netzwerkes zu erhöhen.

16.1. Was ist Kerberos?

Kerberos ist ein von MIT erstelltes Authentifizierungsprotokoll für Netzwerke, das geheime Schlüssel[1] zum Sichern von Passwörtern verwendet — ohne Passwörter über das Netzwerk senden zu müssen. Das Authentifizieren mit Hilfe von Kerberos hält effizient unautorisierte Benutzer vom Versuch ab, Passwörter im Netzwerk abzufangen.

16.1.1. Vorteile von Kerberos

Die meisten herkömmlichen Netzwerksysteme verwenden passwortbasierte Authentifizierungsschemata. Wenn sich ein Benutzer an einem Netzwerkserver anmeldet, muss er einen Benutzernamen und Passwort für jeden Dienst angeben, der Authentifizierung erfordert. Unglücklicherweise erfolgt die Übertragung von Authentifizierungsinformationen bei vielen Diensten im Klartext. Damit ein solches Schemata sicher ist, muss das Netzwerk vor Zugriff von Außen geschützt werden, und alle Computer und Benutzer auf dem Netzwerk müssen sicher sein.

Auch wenn dies der Fall sein sollte, ist das Netzwerk erst einmal mit dem Internet verbunden, kann dessen Sicherheit nicht länger angenommen werden. Jeder Hacker, der Zugriff auf das Netzwerk und einen Paket-Analysierer (Packet Sniffer) hat, kann auf diese Weise versendete Passwörter knacken, was Benutzeraccounts und die Integrität der gesamten Sicherheitsinfrastruktur kompromittiert.

Primäres Ziel von Kerberos ist es, die Übertragung der Authentifizierungsinformationen über das Netzwerk zu beseitigen. Die richtige Verwendung von Kerberos vermindert spürbar die Gefahr, die Packet-Sniffer andernfalls für das Netzwerk bedeuten.

16.1.2. Nachteile von Kerberos

Dank Kerberos wird eine Bedrohung, die ganz allgemein für die Sicherheit im Netzwerk besteht, ausgeschaltet. Allerdings kann sich die Implementierung aus folgenden Gründen schwierig gestalten:

- Das Migrieren von Benutzerpasswörtern von einer standardmäßigen UNIX-Passwortdatenbank wie zum Beispiel `/etc/passwd` oder `/etc/shadow` in eine Kerberos-Passwortdatenbank kann langwierig sein, da es zum Durchführen dieser Aufgabe keine automatisierten Mechanismen gibt. Detailliertere Informationen finden Sie unter Frage 2.23 in den Kerberos online-FAQ unter:

  http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html

1. Ein Systen, bei dem Client und Server einen allgemeinen Schlüssel teilen, der zur Ver- und Entschlüsselung der Netzwerkkommunikation verwendet wird

- Kerberos ist nur teilweise mit dem Pluggable Authentication Modules-System (PAM-System) kompatibel, das die meisten Red Hat Enterprise Linux-Server verwenden. Weitere Informationen hierzu finden Sie unter Abschnitt 16.4.
- Kerberos nimmt an, dass Sie sichere Hosts auf einem unsicheren Netzwerk verwenden. Seine wichtigste Aufgabe ist es, zu vermeiden, dass Passwörter im Klartext über das Netzwerk versendet werden. Wenn jedoch noch jemand anderes als der richtige Benutzer Zugriff auf den Host hat, der die Tickets zur Authentifizierung ausstellt — *Key Distribution Center* (*KDC*) genannt — besteht die Gefahr, dass das gesamte Kerberos-Authentifizierungssystem kompromittiert wird.
- Damit eine Applikation Kerberos verwenden kann, müssen ihre Quellen so modifiziert werden, dass die geeigneten Aufrufe an die Kerberos-Bibliotheken gesendet werden können. Applikationen, die auf diese Art geändert wurden, werden als *kerberisiert* bezeichnet. Bei einigen Applikationen kann dies aufgrund ihrer Größe oder ihrem Design recht problematisch sein. Für andere Applikationen wiederum muss die Art und Weise geändert werden, in der Server und Clients miteinander kommunizieren. Auch dies kann unter Umständen einen großen Aufwand bedeuten. Hierbei stellen die Closed Source-Applikationen ohne standardmäßigen Kerberos-Support den problematischsten Teil dar.
- Bei Kerberos handelt es sich um eine Alles-oder-Nichts-Lösung. Wenn Kerberos im Netzwerk verwendet werden soll, sind alle unverschlüsselten Passwörter, die an einen nicht-kerberisierten Service übertragen werden, einem Risiko unterlegen. D.h., es ergibt sich für Ihr Netzwerk keinerlei Vorteil aus der Verwendung von Kerberos. Wenn Sie Ihr Netzwerk durch Kerberos sichern möchten, müssen Sie entweder *alle* Client/Server-Applikationen, die Passwörter im Klartext versenden, kerberisieren, oder Sie sollten *keine* dieser Applikationen in Ihrem Netzwerk verwenden.

16.2. Kerberos-Terminologie

Wie jedes andere System verfügt Kerberos über seine eigene Terminologie zur Definition verschiedener Aspekte des Dienstes. Ehe die Funktionsweise des Dienstes erläutert wird, sollten Sie mit folgenden Begriffen vertraut sein.

Authentifizierungs-Server (AS)

> Ein Server, der Tickets für einen gewünschten Service ausstellt, die wiederum an Benutzer für den Zugang zu einem Service weitergegeben werden. Der AS antwortet auf Anfragen von Clients, die keine Berechtigungen haben oder keine versenden. Es wird gewöhnlicherweise für den Zugang zum Ticket-granting Server (TGS) Service verwendet, indem ein Ticket-granting Ticket (TGT) ausgestellt wird. Der AS läuft auf dem gleichen Host wie das Key Distribution Center (KDC).

ciphertext

> Verschlüsselte Daten.

Client

> Ein Objekt im Netzwerk (ein Benutzer, ein Host oder eine Applikation), das von Kerberos ein Ticket erhalten kann.

Berechtigungen

> Ein temporärer Satz an elektronischen Berechtigungsnachweisen, die die Identität eines Client für einen bestimmten Dienst verifizieren. Auch als Ticket bezeichnet.

Credential-Cache oder Ticket-Datei

Eine Datei, die die Schlüssel zum Verschlüsseln der Kommunikation zwischen einem Benutzer und verschiedenen Netzwerkdiensten enthält. Kerberos 5 unterstützt einen Rahmen für die Verwendung anderer Cache-Typen wie zum Beispiel gemeinsam genutzten Speicher. Die Dateien werden allerdings besser unterstützt.

Crypt-Hash

Ein unidirektionaler Hash, der zum Authentifizieren von Benutzern verwendet wird. Auch wenn dies sicherer als unverschlüsselte Daten ist, ist das Entschlüsseln für einen erfahrenen Hacker ein Kinderspiel.

GSS-API

Das Generic Security Service Application Program Interface (definiert in RFC-2743 und herausgegeben von der Internet Engineering Task Force) ist eine Sammlung von Funktionen, die Sicherheitsservices bereitstellen. Clients können mit diesenFunktionen Services authentifizieren, und genauso können Services Clients authentifizieren, ohne das diese Programme ein spezifisches Wissen der zugrundeliegenden Mechanismen benötigen. Sollte ein Netzwerk-Service (wie IMAP) die GSS-API verwenden, kann dieser mittels Kerberos authentifizieren.

Hash

Eine Zahl, die aus Text generiert wurde, und dazu verwendet wird, sicherzustellen, dass die übertragenen Daten nicht kompromittiert wurden.

Key (Schlüssel)

Daten, die zum Verschlüsseln bzw. Entschlüsseln von Daten verwendet werden. Verschlüsselte Daten lassen sich ohne den richtigen Schlüssel nicht bzw. nur durch wirklich leistungfähige Programme zum Herausfinden von Passwörtern entschlüsseln.

Key Distribution Center (KDC)

Ein Dienst, der Kerberos-Tickets ausgibt, und normalerweise auf dem gleichen Host wie der Ticket Granting Server (TGS) ausgeführt wird.

Key Table oder Keytab

Eine Datei, die eine unverschlüsselte Liste aller Principals und ihrer Schlüssel enthält. Server holen sich die benötigten Keys aus keytab-Dateien, statt `kinit` zu verwenden. Die standardmäßige keytab-Datei ist `/etc/krb5.keytab`, wobei `/usr/kerberos/sbin/kadmind` der einzige bekannte Service ist, der eine andere Datei verwendet (er verwendet `/var/kerberos/krb5kdc/kadm5.keytab`).

`kinit`

Der Befehl `kinit` erlaubt einem Principal, der bereits angemeldet ist, das anfängliche Ticket Granting Ticket (TGT) zu erhalten und im Cache abzulegen. Weitere Informationen zur Verwendung des Befehls `kinit` finden Sie auf dessen man-Seite.

Principal

Der Principal Name oder Principal ist ein eindeutiger Name für einen Benutzer oder Service, der sich mit Hilfe von Kerberos authentifizieren kann. Der Name eines Principal hat das Format `root[/instance]@REALM`. Bei einem typischen Benutzer entspricht root der Login-ID, während `instance` optional ist. Wenn der Principal über eine Instanz verfügt, ist diese von root durch einen Schrägstrich ("/") getrennt. Bei einem leerem String ("") handelt es sich zwar um eine gültige Instanz (die sich von der Standardinstanz *NULL* unterscheidet), allerdings kann deren Verwendung zu Verwirrung führen. Alle Principals innerhalb eines Realms verfügen über

einen eigenen Schlüssel, der sich für Benutzeraus derem Passwort ableitet oder bei Services nach dem Zufallsprinzip erzeugt wird.

Realm

Ein Netzwerk, das Kerberos verwendet und aus einem oder einigen Servern (auch als KDCs bezeichnet) sowie einer potenziell sehr großen Zahl von Clients besteht.

Service

Ein Programm, auf das über das Netzwerk zugegriffen wird.

Ticket

Ein temporärer Satz elektronischer Berechtigungsnachweise, die die Identität eines Client für einen bestimmten Dienst verifizieren. Auch Berechtigungsnachweis genannt.

Ticket Granting Server (TGS)

Ein Server, der Benutzern der Reihe nach Tickets für den Zugriff auf den gewünschten Service ausgibt. TGS wird üblicherweise auf demselben Host wie KDC ausgeführt.

Ticket Granting Ticket (TGT)

Ein spezielles Ticket, das es dem Client ermöglicht, zusätzliche Tickets zu erhalten, ohne diese beim KDC anfordern zu müssen.

Unverschlüsseltes Passwort

Ein im Klartext lesbares Passwort.

16.3. Funktionsweise von Kerberos

Kerberos unterscheidet sich von Benutzername/Passwort-Authentifizierungsmethoden. Die Authentifizierung erfolgt nicht von jedem Benutzer zu jedem Netzwerk-Service. Kerberos verwendet stattdessen die symmetrische Verschlüsselung und einen vertrauenswürdigen Dritten — das so genannte Key Distribution Center (KDC) — um Benutzer auf einem Netzwerk für mehrere Dienste zu authentifizieren. Nach der Authentifizierung speichert Kerberos ein für diese Sitzung spezifisches Ticket auf dem Rechner des Benutzers. Kerberisierte Dienste suchen dieses Ticket, bevor sie den Benutzer zur Authentifizierung mittels eines Passwortes auffordern.

Wenn sich ein Benutzer in einem kerberisierten Netzwerk an seiner Workstation anmeldet, wird sein Principal für die Anforderung eines Ticket Granting Ticket (TGT) an den Authentifizierungs-Server (AS) gesendet. Diese Anforderung kann entweder vom Anmeldeprogramm (also für den Benutzer transparent) oder nach dem Anmelden des Benutzers vom Programm `kinit` gesendet werden.

Der KDC sucht dann in seiner Datenbank nach diesem Principal. Sobald der Principal gefunden wurde, erstellt der KDC ein TGT, verschlüsselt es unter Verwendung des zu diesem Benutzer gehörenden Schlüssels und sendet es an den Benutzer zurück.

Das Anmeldeprogramm auf dem Client oder `kinit` entschlüsselt das TGT mit Hilfe des Benutzerschlüssels (den es aus dem Passwort des Benutzers errechnet). Der Benutzerschlüssel wird lediglich auf der Client-Maschine benutzt und wird *nicht* über das Netzwerk versendet.

Das TGT ist nur eine bestimmte Zeitspanne (gewöhnlich 10 Stunden) gültig und wird im Berechtigungs-Cache des Client gespeichert. Die Gültigkeitsdauer ist so eingerichtet, dass ein TGT immer nur für eine bestimmte Zeitspanne verwendet werden kann. Ist das TGT erst einmal erstellt, muss der Benutzer das Passwort bis zum Ablauf der Gültigkeit des TGT nicht erneut eingeben bzw. bis sich der Benutzer ab- und neu anmeldet.

Wenn der Benutzer auf einen Netzwerkdienst zugreifen möchte, verwendet der Client das TGT, um vom Ticket Granting Server (TGS) ein Ticket für den Service anzufordern. Der TGS stellt ein Ticket für den gewünschten Service aus, das zur Authentifizierung des Benutzers verwendet wird.

Warnung

Das Kerberos-System kann immer dann kompromittiert werden, wenn ein Benutzer auf dem Netzwerk gegen einen nicht kerberisierten Service authentifiziert und ein Passwort als Klartext gesendet wird. Von der Verwendung von nicht kerberisierten Services wird daher abgeraten. Diese Services umfassen Telnet und FTP. Andere, verschlüsselte Protokolle wie zum Beispiel SSH oder SSL Secured Services können dagegen verwendet werden, auch wenn diese nicht unbedingt ideal sind.

Dies ist selbstverständlich nur ein grober Überblick über die typische Funktionsweise der Kerberos-Authentifizierung in einem Netzwerk. Weiterführende Informationen zur Kerberos-Authentifizierung finden Sie unter Abschnitt 16.7.

Anmerkung

Kerberos benötigt verschiedene Netzwerk-Services, um fehlerfrei zu arbeiten. Zunächst ist für Kerberos eine Zeitsynchronisierung zwischen den Rechnern im Netzwerk erforderlich. Für das Netzwerk sollte daher ein Programm zur Zeitsynchronisierung wie zum Beispiel `ntpd` eingerichtet werden. Weiterführende Informationen zum Konfigurieren von `ntpd` und zum Einrichten von NTP (Network Time Protocol) Servern finden Sie unter `/usr/share/doc/ntp-`<*version-number*>`/index.htm` (ersetzen Sie <*version-number*> durch die Versionsnummer des auf Ihrem System installierten `ntp`-Pakets).

Da Kerberos zum Teil auch auf den Domain Name Service (DNS) angewiesen ist, müssen Sie sich außerdem vergewissern, dass die DNS-Einträge und Hosts im Netzwerk richtig eingerichtet sind. Weitere Informationen finden Sie im*Kerberos V5 System Administrator's Guide*, der unter `/usr/share/doc/krb5-server-`<*version-number*> in den Formaten PostScript und HTML zur Verfügung steht (ersetzen Sie <*version-number*> mit der Versionsnummer des auf Ihrem System installierten `krb5-server`-Paket.

16.4. Kerberos und PAM

Derzeit verwenden die kerberisierten Dienste keinerlei PAM (Pluggable Authentication Modules) — Kerberisierte Server überspringen PAM vollständig. Applikationen, die PAM verwenden, können Kerberos jedoch zur Authentifizierung nutzen, sofern das Modul `pam_krb5` (im Paket `pam_krb5` enthalten) installiert ist. Das Das Paket `pam_krb5` enthält Beispielkonfigurationsdateien, durch die Dienste wie `login` und `gdm` in der Lage sind, Benutzer zu authentifizieren und unter Verwendung ihrer Passwörter erste Berechtigungsnachweise zu erhalten. Unter der Voraussetzung, dass der Zugriff auf Netzwerkserver immer über kerberisierte Dienste oder über Dienste vorgenommen wird, die GSS-API verwenden, wie z.B. IMAP, kann das Netzwerk als relativ sicher bezeichnet werden.

Tipp

Administratoren sollten vorsichtig sein, es Benutzern nicht zu erlauben zu den meisten Services mit Kerberos-Passwörtern zu authentifizieren. Viele der von diesen Services verwendeten Protokolle verschlüsseln die Passwörter nicht, bevor sie diese über das Netzwerk versenden. Dies hebt die Vorteile eines Kerberos Systems auf. Benutzern sollte es, zum Beispiel, nicht erlaubt sein, deren Kerberos-Passwörter über Telnet zu authentifizieren.

16.5. Konfigurieren eines Kerberos 5-Servers

Installieren Sie zuerst den Server, wenn Sie Kerberos einrichten. Wenn Sie Slave-Server einrichten müssen, finden Sie Detailinformationen zum Festlegen der Beziehungen zwischen den Master- und Slave-Servern im *Kerberos 5 Installation Guide* im Verzeichnis `/usr/share/doc/krb5-server-<Versionsnummer>` (ersetzen Sie *<version-number>* mit der Versionsnummer des auf Ihrem System installierten `krb5-server`-Pakets).

Führen Sie diese Schritte aus, um einen Kerberos-Server zu konfigurieren:

1. Stellen Sie sicher, dass die Zeitsynchronisierung und DNS auf dem Server funktionieren, ehe Sie Kerberos 5 konfigurieren. Schenken Sie der Zeitsynchronisierung zwischen dem Kerberos-Server und seinen verschiedenen Clients besondere Aufmerksamkeit. Überschreitet die Zeitdifferenz zwischen der Server- und den Clientuhren fünf Minuten (der Standardwert kann in Kerberos 5 konfiguriert werden), sind die Kerberos-Clients nicht in der Lage, sich am Server anzumelden. Diese Zeitsynchronisierung ist notwendig, um Angreifer davon abzuhalten, ein altes Kerberos-Ticket zu verwenden, um sich als gültigen Benutzer auszugeben.

   Selbst wenn Sie Kerberos nicht verwenden, sollten Sie ein NTP-kompatibles Client-Server-Netzwerk einrichten. Red Hat Enterprise Linux beeinhaltet hierfür das `ntp`-Paket. Weitere Informationen finden Sie unter `/usr/share/doc/ntp-<version-number>/index.htm` zum Einrichten eines NTP Servers und http://www.eecis.udel.edu/~ntp für zusätzliche Informationen zu NTP.

2. Installieren Sie auf dem dafür abgestellten Rechner, auf dem KDC ausgeführt wird, die Pakete `krb5-libs`, `krb5-server` und `krb5-workstation`. Dieser Rechner muss extrem sicher sein — wenn möglich, sollten außer KDC keine anderen Services ausgeführt werden.

   Wenn Sie Kerberos mit einem GUI-Utility verwalten möchten, sollten Sie auch das `gnome-kerberos`-Paket installieren. Es enthält `krb5`, ein GUI-Tool zum Verwalten von Tickets.

3. Bearbeiten Sie die Konfigurationsdateien `/etc/krb5.conf` und `/var/kerberos/krb5kdc/kdc.conf`, um den Realm-Namen sowie die Domain-Realm-Zuordnungen anzugeben. Ein einfacher Realm kann durch das Ersetzen von Instanzen von *`BEISPIEL.COM`* und *`Beispiel.com`* durch Ihren Domainnamen erstellt werden — beachten Sie die Groß- und Kleinschreibung — sowie durch Ändern des KDC von *`Kerberos.Beispiel.com`* in den Namen des Kerberos-Servers. Hierbei gilt, dass alle Realm-Namen groß und alle DNS-Hostnamen und Domainnamen klein geschrieben werden. Weitere Informationen zum Format dieser Dateien finden Sie auf den jeweiligen man-Seiten.

4. Erstellen Sie die Datenbank mit Hilfe des Dienstprogramms `kdb5_util` von einem Shell-Prompt:

   ```
   /usr/kerberos/sbin/kdb5_util create -s
   ```

   Der Befehl `create` erstellt die Datenbank, die zum Speichern der Schlüssel für den Kerberos-Realm verwendet wird. Der Switch `-s` erzwingt die Erstellung einer *stash*-Datei, in der der Master-Server-Schlüssel gespeichert wird. Ist keine stash-Datei vorhanden, von der der Schlüssel gelesen werden kann, fordert der Kerberos-Server (`krb5kdc`) die Benutzer bei jedem Start zur Eingabe des Passwortes des Master-Servers auf (wodurch der Schlüssel erneut generiert werden kann).

5. Bearbeiten Sie die Datei `/var/kerberos/krb5kdc/kadm5.acl`. Diese Datei wird von `kadmind` zum Ermitteln der Principals mit Zugriff auf die Kerberos-Datenbank sowie deren Zugriffslevel verwendet. Die meisten Organisationen kommen mit einer einzigen Zeile aus:

   ```
   */admin@EXAMPLE.COM  *
   ```

Die meisten Benutzer werden in der Datenbank durch einen einzelnen Principal dargestellt (mit einer *NULL* oder leeren Instanz wie zum Beispiel *joe@EXAMPLE.COM*). Mit dieser Konfiguration können Benutzer mit einem zweiten Principal mit einer *admin*-Instanz (zum Beispiel *joe/admin@EXAMPLE.COM*) kompletten Zugriff auf die Kerberos-Datenbank des Realm erhalten.

Sobald `kadmind` auf dem Server gestartet ist, können alle Benutzer auf die Dienste zugreifen, indem sie auf einem beliebigen Client oder Server im Realm `kadmin` ausführen. Allerdings können nur die in der Datei `kadm5.acl` genannten Benutzer die Datenbank ändern, ausgenommen das eigene Passwort.

Anmerkung

Das `kadmin`-Utility kommuniziert mit dem `kadmind`-Server über das Netzwerk, wobei Kerberos für die Authentifizierung verwendet wird. Sie müssen natürlich den ersten Principal erstellen, ehe Sie eine Verbindung mit dem Server über das Netzwerk herstellen können, um diesenzu verwalten. Erstellen Sie den ersten Principal mit dem Befehl `kadmin.local`, der speziell für den Gebrauch auf demselben Host wie KDC entworfen ist und Kerberos nicht zur Authentifizierung verwendet.

Geben Sie am KDC-Terminal den folgenden `kadmin.local`-Befehl ein, um den ersten Principal zu erstellen:

```
/usr/kerberos/sbin/kadmin.local -q "addprinc username/admin"
```

6. Starten Sie Kerberos mit Hilfe der folgenden Befehle:

```
/sbin/service krb5kdc start
/sbin/service kadmin start
/sbin/service krb524 start
```

7. Fügen Sie Principals für Ihre Benutzer mit Hilfe des Befehls `addprinc` mit `kadmin` hinzu. `kadmin` und `kadmin.local` auf dem Master-KDC sind die Befehlszeilenschnittstellen zum KDC. Insofern stehen viele Befehle nach dem Starten des `kadmin`-Programms zur Verfügung. Weitere Informationen finden Sie auf der man-Seite zu `kadmin`.

8. Überprüfen Sie, ob das KDC Tickets ausgibt. Führen Sie zuerst `kinit` aus, um ein Ticket zu erhalten, und speichern Sie es in einer Credential-Cache-Datei. Zeigen Sie dann mit `klist` eine Referenzenliste im Cache an und verwenden Sie `kdestroy`, um den Cache sowie die enthaltenen Referenzen zu zerstören.

Anmerkung

Standardmäßig versucht `kinit`, Sie mit Hilfe des Anmeldenamens des Kontos zu authentifizieren, das Sie zur ersten Anmeldung am System verwendeten (nicht am Kerberos-Server). Entspricht der Systembenutzername keinem Principal in der Kerberos- Datenbank, gibt `kinit` eine Fehlermeldung aus. Geben Sie in diesem Fall `kinit` den Namen Ihres Principal als Argument auf der Befehlszeile an (`kinit <principal>`).

Wenn Sie oben genannte Schritte ausgeführt haben, sollte Ihr Kerberos-Server korrekt funktionieren.

16.6. Konfigurieren eines Kerberos 5-Clients

Das Einrichten eines Kerberos 5-Client ist wesentlich einfacher als das Einrichten eines Servers. Sie sollten zumindest die Clientpakete installieren und den Clients eine gültige `krb5.conf`-Konfigurationsdatei zur Verfügung stellen. Kerberisierte Versionen von `rsh` und `rlogin` erfordern ebenfalls einige Konfigurationsänderungen.

1. Stellen Sie sicher, dass zwischen dem Kerberos-Client und KDC Zeitsynchronisierung vorhanden ist. Weitere Informationen finden Sie unter Abschnitt 16.5. Zudem sollten Sie prüfen, dass DNS auf dem Kerberos-Client fehlerfrei läuft, bevor die Kerberos-Clientprogramme installiert werden.
2. Installieren Sie die Pakete `krb5-libs` und `krb5-workstation` auf allen Client-Rechnern. Für jeden Client müssen Sie eine gültige Version von `/etc/krb5.conf` zur Verfügung stellen (dies kann normalerweise dieselbe `krb5.conf`-Datei sein, die von KDC verwendet wird).
3. Ehe eine bestimmte Workstation im Realm Benutzern das Herstellen einer Verbindung mit Hilfe der kerberisierten Befehle `rsh` und `rlogin` erlaubt, muss auf der Workstation zum einen das `xinetd`-Paket installiert sein und zum anderen muss sie ihren eigenen Hostprincipal in der Kerberos-Datenbank haben. Die Serverprogramme `kshd` und `klogind` benötigen ebenfalls Zugriff auf die Schlüssel für den Principal ihres Services.

   Mit Hilfe von `kadmin` fügen Sie einen Hostprincipal für die Workstation auf dem KDC hinzu. Die Instanz ist in diesem Fall der Hostname der Workstation. Sie können die Option `-randkey` für den `kadmin`-Befehl `addprinc` verwenden, um den Principal zu erstellen und ihm einen zufällig ausgewählten Schlüssel zuweisen:

   ```
   addprinc -randkey host/blah.example.com
   ```

   Nachdem der Principal erstellt ist, können Sie die Schlüssel für die Workstation extrahieren, indem Sie `kadmin` *auf der Workstation selbst* ausführen und den Befehl `ktadd` in `kadmin` verwenden:

   ```
   ktadd -k /etc/krb5.keytab host/blah.example.com
   ```

4. Sollten Sie andere kerberisierten Netzwerk-Services benutzen wollen, müssen diese gestartet werden. Folgend ist eine Liste der gebräuchlicheren kerberisierten Services und Anleitungen zum Aktivieren dieser:

   - `rsh` und `rlogin` — Um die kerberisierten Versionen von `rsh` und `rlogin` zu verwenden, müssen Sie `klogin`, `eklogin` und `kshell` aktivieren.
   - Telnet — Um das kerberisierte Telnet verwenden zu können, müssen Sie `krb5-telnet` aktivieren.
   - FTP — Zum Bereitstellen von FTP-Zugriff müssen Sie einen Schlüssel für einen Principal mit einem root von `ftp` erstellen und extrahieren. Dabei muss die Instanz auf den Hostnamen des FTP-Servers festgelegt sein. Aktivieren Sie dann `gssftp`.
   - IMAP — Der IMAP-Server, im `imap`-Paket enthalten, verwendet die GSS-API-Authentifizierung unter Verwendung von Kerberos 5, wenn es den richtigen Key in `/etc/krb5.keytab` findet. Der root für den Principal sollte `imap` sein.
   - CVS — CVSs kerberisierter `gserver` verwendet einen Principal mit `cvs` als root. Andernfalls stimmt er mit `pserver` überein.

   Detaillierte Informationen zum Aktivieren von Services finden Sie im Kapitel *Zugriffskontrolle für Dienste* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

16.7. Zusätzliche Ressourcen

Weitere Informationen zu Kerberos finden Sie in folgenden Ressourcen.

16.7.1. Installierte Dokumentation

- Im Verzeichnis `/usr/share/doc/krb5-server-<version-number>` — Die *Kerberos V5 Installation Guide* und die *Kerberos V5 System Administrator's Guide* in den Formaten PostScript und HTML. Das `krb5-server`-Paket muss installiert sein.

- Im Verzeichnis `/usr/share/doc/krb5-workstation-<version-number>` — Der *Kerberos V5 UNIX User's Guide* in den Formaten PostScript und HTML. Das `krb5-workstation`-Paket muss installiert sein.
- Kerberos man-Seiten — Es gibt eine Vielzahl von man-Seiten für die verschiedenen Applikationen und Konfirgurationsdateien für die Implementation von Kerberos. Im folgenden finden Sie eine Liste der bedeutenderen man-Seiten.

Client-Applikationen

- `man kerberos` — Eine Einführung in das Kerberos-System, in dem beschrieben wird, wie Berechtigungsnachweise funktionieren, und Empfehlungen für das Erhalten und Löschen von Kerberos-Tickets ausgegeben werden. Unten auf der man-Seite werden verwandte man-Seiten angegeben.
- `man kinit` — Beschreibt, wie man diesen Befehl für das Erhalten und Cachen eines Ticket-Granting Tickets verwendet.
- `man kdestroy` — Beschreibt, wie man diesen Befehl zum Löschen von Kerberos-Berechtigungsnachweisen verwendet.
- `man klist` — Beschreibt, wie man diesen Befehl zum Auflisten von gecachten Kerberos-Berechtigungsnachweisen verwendet.

Administrative Applikationen

- `man kadmin` — Beschreibt, wie man diesen Befehl zur Verwaltung der Kerberos V5 Datenbank verwendet.
- `man kdb5_util` — Bechreibt, wie man diesen Befehl zum Erstellen und Durchführen administrativer Funktionen in der Kerberos V5 Datenbank verwendet.

Server Applikationen

- `man krb5kdc` — Beschreibt die zur Verfügung stehenden Befehlszeilenoptionen für das Kerberos V5 Key Distribution Center.
- `man kadmind` — Beschreibt die zur Verfügung stehenden Befehlszeilenoptionen für den Kerberos V5 Administration Server.

Konfirgurationsdateien

- `man krb5.conf` — Beschreibt das Format und die zur Verfügung stehenden Optionen innerhalb der Konfigurationsdatei der Kerberos V5 Bibliothek.
- `man kdc.conf` — Beschreibt das Format und die zur Verfügung stehenden Optionen innerhalb der Konfigurationsdatei der Kerberos V5 Authentication Server (AS) und Key Distribution Center (KDC).

16.7.2. Hilfreiche Webseiten

- http://web.mit.edu/kerberos/www — *Kerberos: The Network Authentication Protocol* Webseite vom MIT.
- http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html — Die Seite mit den am häufigsten gestellten Fragen zu Kerberos (Frequently Asked Questions - FAQ).
- ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS — Die PostScript-Version von *Kerberos: An Authentication Service for Open Network Systems* von Jennifer G. Steiner, Clifford Neuman und Jeffrey I. Schiller. Dieses Dokument ist die Originalbeschreibung zu Kerberos.
- http://web.mit.edu/kerberos/www/dialogue.html — *Designing an Authentication System: a Dialogue in Four Scenes* 1988 von Bill Bryant verfasst, 1997 von Theodore Ts'o überarbeitet. Das Dokument enthält ein Gespräch zwischen zwei Entwicklern, die über die Schaffung eines Authentifizierungssystems in der Art von Kerberos nachdenken. Dank seines Gesprächscharakters und dadurch, dass zunächst die Grundlagen diskutiert werden, eignet sich dieses Dokument besonders für Benutzer, die noch nicht mit Kerberos vertraut sind.
- http://www.ornl.gov/~jar/HowToKerb.html — *How to Kerberize your site* ist eine gute Referenz zur Kerberisierung eines Netzwerks.
- http://www.networkcomputing.com/netdesign/kerb1.html — *Kerberos Network Design Manual* gibt eine ausführliche Übersicht über Kerberos.

Kapitel 17.

SSH-Protokoll

SSH™ (oder *S*ecure *SH*ell) ist ein Protokoll, das die sichere Kommunikation zwischen zwei Systemen mittels einer Client/Server Architektur ermöglicht, und über das Benutzer sich entfernt in ein Server-Host-System einloggen können.Im Gegensatz zu anderen Remote-Kommunikationsprotokollen wie FTP oder Telnet, verschlüsselt SSH die Anmeldung. Auf diese Weise können Eindringlinge keine unverschlüsselten Passwörter erkennen.

SSH wurde als Ersatz für ältere, weniger sichere Terminalanwendungen, die zum Anmelden in Remote-Hosts wie `telnet` oder `rsh` verwendet werden, entwickelt. Das Programm `scp` ersetzt ältere Programme wie **rcp**, die zum Kopieren von Dateien zwischen Hosts verwendet wurden. Da diese älteren Programme Passwörter zwischen dem Client und dem Server nicht verschlüsseln, sollten Sie möglichst vermeiden, diese zu verwenden. Die Verwendung von sicheren Methoden zum Anmelden verringert das Sicherheitsrisiko des Client- und des Host-Systems.

17.1. SSH-Merkmale

Das SSH-Protokoll liefert folgende Schutzmöglichkeiten:

- Nach einer ersten Verbindung prüft der Client, ob er sich auch in der Folge mit dem gleichen Server verbindet.
- Der Client überträgt die Authentifizierungsinformationen in verschlüsselter Form an den Server, unter Verwendung von 128-Bit Verschlüsselung.
- Alle während der Verbindung gesendeten und empfangenen Daten sind mit der 128 Bit-Verschlüsselung so komplex verschlüsselt, dass es äußerst schwierig ist, abgefangene Übertragungen zu entschlüsseln und zu lesen.
- Der Client kann X11 [1] Applikationen vom Server weiterleiten. Diese Technik, *X11 forwarding* genannt, gewährleistet die sichere Verwendung grafischer Applikationen über ein Netzwerk.

Das das SSH Protokoll alles verschlüsselt, das gesendet oder empfangen wird, können damit auch unsichere Protokolle verschlüsselt werden. Mit *port forwarding* kann ein SSH Server zum Verschlüsseln unsicherer Protokolle, z.B.POP, verwendet werden und somit die Sicherheit des Systems und der Daten erhöhen.

Red Hat Enterprise Linux enthält die allgemeinen OpenSSH Pakete (`openssh`), den OpenSSH Server (`openssh-server`) und Client (`openssh-clients`)-Pakete. Weitere Informationen über die Installation und den Einsatz von OpenSSH finden Sie im Kapitel *OpenSSH* des *Red Hat Enterprise Linux Handbuch zur System-Administration*. Bitte beachten Sie, dass die OpenSSH-Pakete das OpenSSL-Paket (`openssl`) erfordern. OpenSSL installiert verschiedene wichtige kryptographische Bibliotheken, die OpenSSH bei der Erstellung mit verschlüsselten Meldungen unterstützt.

17.1.1. Wozu dient SSH?

Skrupellosen Computerbenutzern stehen eine Reihe von Tools zur Verfügung, um die Netzwerkkommunikation zu stören, abzufangen und umzuleiten und um auf diese Weise Zugriff auf Ihr System zu erhalten. Diese Gefahren können generell wie folgt klassifiziert werden:

1. X11 bezieht sich auf das X11R6 Anzeigesystem, das gewöhnlich als X Window System oder X bezeichnet wird. Red Hat Enterprise Linux enthält XFree86, ein Open Source X Window System.

- *Abfangen von Mitteilungen zwischen zwei Systemen* — In diesem Fall gibt es irgendwo im Netzwerk zwischen den miteinander kommunizierenden Systemen einen Dritten, der die Informationen, die zwischen den beiden Systemen ausgetauscht werden, kopiert. Der Dritte kann dabei die Informationen abfangen und aufbewahren oder sie auch ändern und an den eigentlichen Empfänger weiterleiten.

  Dieser mögliche Angriff kann durch die Verwendung eines Packet-Sniffers — einem gewöhnlichen Netzwerk-Dienstprogramm gemountet werden.

- *Imitation eines bestimmten Hosts* — Mit dieser Strategie ist ein drittes System so konfiguriert, dass es vorgibt, der eigentliche Empfänger einer Übertragung zu sein. Ist die Strategie erfolgreich, bemerkt das Benutzersystem nicht, dass es mit dem falschen Host kommuniziert.

  Dieser mögliche Angriff kann anhand von Techniken, die unter dem Namen DNS-Poisoning [2] oder IP-Spoofing [3] bekannt sind, gemounted werden.

Bei beiden Methoden werden möglicherweise wichtige Informationen abgefangen. Wenn dies aus unlauteren Gründen erfolgt, können die Ergebnisse katastrophal sein.

Wenn SSH für Fernanmeldungen über eine Shell und für das Kopieren von Dateien verwendet wird, können diese Sicherheitsrisiken erheblich gemindert werden. Das ist darauf zurückzuführen, dass der SSH-Client und Server digitale Unterschriften verwenden, um gegenseitig ihre Identität zu prüfen. Außerdem sind alle Mitteilungen zwischen Client und Server verschlüsselt. Dabei nutzen auch Versuche, sich als das eine oder andere System auszugeben, nichts, da der Schlüssel hierfür nur dem lokalen und dem remote-System bekannt ist.

17.2. SSH Protokoll Versionen

Das SSH-Protokoll erlaubt jedem Client- und Server-Programm, welches zu den Spezifikationen des Protokolls gebaut wurde, sicher zu kommunizieren und austauschbar verwendet werden zu können.

Zur Zeit gibt es zwei Versionen von SSH. SSH Version 1 verwendet verschiedene patentierte Verschlüsselungsalgorithmen (einige dieser Patente sind allerdings abgelaufen), hat allerdings ein Sicherheitsrisiko, das unter Umständen erlaubt, Daten in den Datenfluss einzufügen. Die OpenSSH-Suite unter Red Hat Enterprise Linux verwendet standardmäßig SSH Version 2, da diese Version des Protokolls einen erweiterten Algorithmus für den Schlüsselaustausch besitzt, der nicht so anfällig ist. Die OpenSSH-Suite unterstützt jedoch auch weiterhin SSH1 Verbindungen.

Wichtig

Es ist empfohlen nur SSH Version 2-kompatible Server und Clients zu verwenden, sofern dies möglich ist.

17.3. Die Abfolge der Vorgänge einer SSH-Verbindung

Die folgende Abfolge von Vorgängen tragen zu einer unversehrten SSH-Kommunikation zwischen zwei Hosts bei:

2. DNS-Poisoning erfolgt, wenn ein Eindringling einen DNS-Server knackt und Client-Systeme auf einen böswillig vervielfältigten Host zu lenken.
3. IP-Spoofing erfolgt, wenn ein Eindringling Netzwerk-Pakete versendet, die scheinbar von einem vertrauenswürdigen Host auf dem Netzwerk versendet werden.

- Zunächst wird eine sichere Transportschicht geschaffen, die dem Client-System anzeigt, dass es mit dem korrekten Server in Verbindung steht.
- Die Transportschicht zwischen dem Client und dem Remote-Host ist mit einer symmetrischen Kodierung verschlüsselt.
- Der Client authentifiziert sich gegenüber dem Server.
- Der Remote-Client kann nun sicher mit dem Remote-Host über die verschlüsselte Verbindung kommunizieren.

17.3.1. Transportschicht

Die wichtigste Aufgabe der Transportschicht ist es, die sichere und verschlüsselte Kommunikation zwischen zwei Rechnern bei und nach der Authentifizierung zu gewährleisten. Die Transportschicht verwaltet zu diesem Zweck die Verschlüsselung und Entschlüsselung der Daten und sorgt dafür, dass die Datenpakete während des gesamten Übertragungsflusses geschützt sind. Weiterhin kann diese Schicht die Daten komprimieren und damit die Übertragungsgeschwindigkeit erheblich erhöhen.

Sobald ein Client über ein SSH-Protokoll mit einem Server in Verbindung tritt, erfolgen verschiedene wichtige Vorgänge, die dazu dienen, dass die beiden Systeme die Transportschicht korrekt aufbauen:

- Austausch der Schlüssel
- Zu verwendenden Algorithmus für den öffentlichen Schlüssel bestimmen
- Zu verwendenden Algorithmus für die symmetrische Verschlüsselung bestimmen
- Zu verwendenden Algorithmus für die Authentifizierung der Mitteilungen bestimmen
- Der Hash-Algorithmus wird bestimmt

Beim Austausch der Schlüssel identifiziert sich der Server gegenüber dem Client mithilfe eines eindeutigen *Host-Schlüssel*. Hat der Client bisher noch nie mit diesem Server kommuniziert, ist der Server-Schlüssel dem Client unbekannt und es wird keine Verbindung hergestellt. OpenSSH umgeht dieses Problem, indem es den Host-Schlüssel des Servers akzeptiert, nachdem der Benutzer benachrichtigt wurde und prüft die Akzeptanz des neuen Host-Schlüssels. Bei allen nachfolgenden Verbindungen wird dieser Schlüssel mit der gespeicherten Version des Clients verglichen und auf diese Weise sichergestellt, dass der Client tatsächlich mit dem gewünschten Server kommuniziert. Sollte der Host-Schlüssel in Zukunft nicht mehr passen, muss der Benutzer die gespeicherte Version des Client entfernen, bevor eine Verbindung zustande kommen kann.

Achtung

Es ist möglich, dass ein Hacker sich zum Beispiel bei der ersten Verbindung als Server ausgeben kann, da der lokale Rechner zu diesem Zeitpunkt den gewünschten Server und einen unerlaubt eingerichteten Server noch nicht unterscheiden kann. Um dies zu vermeiden, sollten Sie die Integrität eines neuen SSH-Servers prüfen, indem Sie sich vor dem ersten Kontakt oder nachdem sich der Host-Schlüssel geändert hat, mit dem Server-Administrator in Verbindung setzen.

Das SSH-Protokoll wurde konzipiert, um mit fast allen Algorithmen oder Formaten für allgemeine Schlüssel verwendet werden zu können. Nachdem ein erster Schlüsselaustausch zwei Werte erstellt hat (einen Hash-Wert für den Austausch und einen gemeinsam genutzten, geheimen Wert), berechnen die beiden Systeme sofort neue Schlüssel und Algorithmen, um die Authentifizierung und die in der Folge über die Verbindung gesendeten Daten zu schützen.

Nachdem eine bestimmte Datenmenge mithilfe eines vorgegebenen Schlüssels und Algorithmus übertragen wurde (die genaue Menge hängt von der SSH-Implementation ab), erfolgt ein weiterer Schlüsselaustausch, der wiederum einen neuen Hash-Wert und einen neuen, gemeinsam genutzten, geheimen

Wert generiert. Auch wenn eine unbefugte Person diese beiden Werte ermitteln sollte, müsste sie diese Information bei jedem neuen Schlüsselaustausch ermitteln, um die Verbindung zu überwachen.

17.3.2. Authentifizierung

Nachdem die Transportschicht einen sicheren Kanal geschaffen hat, in dem die Informationen zwischen den beiden Systemen übertragen werden, teilt der Server dem Client die verschiedenen unterstützten Authentifizierungsmethoden mit (beispielsweise eine private, verschlüsselte Signatur oder die Eingabe eines Passworts). Der Client wird anschließend versuchen, sich anhand einer der unterstützten Methoden gegenüber dem Server zu identifizieren.

SSH Server und Clients können konfiguriert werden, um verschiedene Arten der Authentifizierung zu ermöglichen. Diese Methode bietet daher jeder Seite das ideale Maß an Kontrolle. Der Server kann entscheiden, welche Verschlüsselungsmethoden er auf der Grundlage seines Sicherheitsmodells unterstützen möchte, und der Client kann festlegen, in welcher Reihenfolge er die verschiedenen verfügbaren Authentifizierungsmethoden verwendet. Dank der Sicherheit der SSH-Transportschicht sind auch scheinbar unsichere Authentifizierungsmethoden, wie Host- und Passwort-basierte Authentifizierung, sicher.

17.3.3. Verbindungskanäle

Nach der erfolgreichen Authentifizierung über die SSH- Transportschicht werden mehrere *Kanäle* (channels) unter Verwendung von Multiplexing[4] geöffnet. Jeder der Kanäle bearbeitet die Mitteilungen für eine andere Terminal- oder weitergeleitete X11-Sitzung.

Sowohl Clients als auch Server können einen neuen Kanal erstellen, wobei jedem Kanal an jedem Ende eine unterschiedliche Nummer zugewiesen wird. Wenn eine Seite einen neuen Kanal öffnen möchte, wird die Nummer der entsprechenden Seite des Kanals mit der Anforderung übermittelt. Diese Information wird von der anderen Seite gespeichert und verwendet, um eine bestimmte Mitteilung an diesen Kanal weiterzuleiten. Ziel ist zu vermeiden, dass sich verschiedene Arten Sessionen beeinflussen und die Kanäle geschlossen werden können, ohne die primäre SSH-Verbindung zwischen den beiden Systemen zu unterbrechen.

Kanäle unterstützen auch die *Datenflusskontrolle*, was es ihnen ermöglicht, Daten geordnet zu senden und zu empfangen. Auf diese Weise werden Daten erst dann über den Kanal gesendet, wenn der Host-Rechner die Meldung erhält, dass der Kanal empfangsbereit ist.

Der Client und Server übertragen automatisch die Eigenschaften jedes Kanals, je nachdem, welche Art von Dienst der Client abruft und wie der Benutzer mit dem Netzwerk verbunden ist. Dadurch ergibt sich eine größere Flexibilität bei der Handhabung der verschiedenen Arten von Remote-Verbindungen ohne die Basis-Infrastruktur des Protokolls ändern zu müssen.

17.4. OpenSSH-Konfigurationsdateien

OpenSSH verfügt über zwei verschiedene Arten von Konfigurationsdateien: eine für Clientprogramme (`ssh`, `scp`, `sftp`) und eine andere für den Server-Daemon (`sshd`).

Die SSH-Konfigurationsinformationen für das gesamte System sind im Verzeichnis `/etc/ssh` gespeichert:

4. Eine Multiplex-Verbindung besteht aus verschiedenen Signalen, die über ein gemeinsam genutztes Medium gesendet werden. Bei SSH werden verschiedene Kanäle über eine gemeinsame, verschlüsselte Verbindung gesendet.

- `moduli` — Hier sind Diffie-Hellmann Gruppen für den Austausch des Diffie-Hellmann Schlüssels enthalten. Wenn der Austausch dieser Schlüssel zu Beginn einer SSH-Sitzung erfolgt, wird ein gemeinsam genutzter, geheimer Wert erstellt, der von keiner Seite allein erstellt werden kann. Dieser Wert wird zur Host-Authentifizierung verwendet.
- `ssh_config` — Hierbei handelt es sich um eine Datei für die Konfiguration des SSH-Clients. Wenn einem Benutzer eine eigene Konfigurationsdatei in seinem Home-Verzeichnis (`~/.ssh/config`) zur Verfügung steht, werden die hier enthaltenen Werte überschrieben.
- `sshd_config` — Die Konfigurationsdatei für den `sshd` Daemon.
- `ssh_host_dsa_key` — Der private DSA-Schlüssel, der vom `sshd` Daemon verwendet wird.
- `ssh_host_dsa_key.pub` — Der öffentliche DSA-Schlüssel, der vom `sshd` Daemon verwendet wird.
- `ssh_host_key` — Der private RSA Schlüssel, der vom `sshd` Daemon für die Version 1 des SSH-Protokolls verwendet wird.
- `ssh_host_key.pub` — Der öffentliche RSA Schlüssel, der vom `sshd` Daemon für die Version 1 des SSH-Protokolls verwendet wird.
- `ssh_host_rsa_key` — Der private RSA Schlüssel, der von `sshd` Daemon für die Version 2 des SSH-Protokolls verwendet wird.
- `ssh_host_rsa_key.pub` — Der öffentliche RSA Schlüssel, der von `sshd` für die Version 2 des SSH-Protokolls verwendet wird.

Die benutzerspezifischen SSH-Konfigurationsinformationen werden im Home-Verzeichnis des Benutzers im Unterverzeichnis `~/.ssh/` gespeichert:

- `authorized_keys` — In dieser Datei ist eine Liste der autorisierten öffentlichen Schlüssel für Server enthalten. Stellt ein Client eine Verbindung zu einem Server her, wird er von diesem durch Prüfen seines unterschriebenen öffentlichen Schlüssels, der in dieser Datei gespeichert ist, authentifiziert.
- `id_dsa` — Diese Datei enthält den privaten Schlüssel des Benutzers.
- `id_dsa.pub` — Der öffentliche DSA- Schlüssel des Benutzers.
- `id_rsa` — Der private RSA-Schlüssel, welcher von `ssh` für Version 2 des SSH-Protokolls verwendet wird.
- `id_rsa.pub` — Der öffentliche RSA-Schlüssel, welcher von `ssh` für Version 2 des SSH-Protokolls verwendet wird.
- `identity` — Der private RSA-Schlüssel, welcher von `ssh` für Version 1 des SSH-Protokolls verwendet wird.
- `identity.pub` — Der öffentliche RSA-Schlüssel, welcher von `ssh` für Version 1 des SSH-Protokolls verwendet wird.
- `known_hosts` — In dieser Datei können die DSA-Host-Schlüssel der Server gespeichert werden, mit denen sich der Benutzer über SSH anmeldet. Diese Datei ist sehr wichtig, um festzustellen, ob der SSH-Client mit dem richtigen SSH-Server verbunden ist.

Wichtig

Wenn der Host-Schlüssel eines SSH-Servers geändert wurde, wird der Client den Benutzer darauf hinweisen, dass die Verbindung nicht fortgesetzt werden kann, bevor nicht der Host-Schlüssel aus der Datei `known_hosts` gelöscht wurde. Dies kann mit einem Texteditor geschehen. Bevor dies geschieht, sollten Sie sich allerdings zuerst mit dem System-Administrator des SSH-Servers in Verbindung setzen, um sicherzustellen, dass der Server nicht kompromittiert wurde.

Auf den man-Seiten von `ssh_config` und `sshd_config`finden Sie weitere Informationen über die verschiedenen Direktiven in den SSH-Konfigurationsdateien.

17.5. Mehr als eine Secure Shell

Eine sichere Befehlszeilenschnittstelle stellt nur eine der vielen Arten und Weisen dar, wie SSH verwendet werden kann. Mit einer angemessenen Bandbreite können X11-Sitzungen über einen SSH-Kanal verwaltet werden. Mithilfe von TCP/IP-Forwarding können bisher unsichere Port-Verbindungen zwischen Systemen auf spezifische SSH-Kanäle gemappt werden.

17.5.1. X11 Forwarding

Eine X11-Sitzung über eine bestehende SSH-Verbindung zu öffnen ist so einfach wie das Ausführen eines X-Programms, während Sie bereits einen X-Client auf Ihrem Host ausführen. Wird ein X-Programm von einem Secure Shell Prompt ausgeführt, erstellen der SSH-Client und -Server einen neuen, verschlüsselten Kanal in der aktuellen SSH-Verbindung, und die Daten des X-Programms werden über diesen Kanal auf Ihren Client-Rechner gesendet.

Sie können sich sicherlich vorstellen, wie nützlich X11-Forwarding sein kann. Sie können hiermit zum Beispiel eine sichere, interaktive Sitzung mithilfe von `up2date` auf dem Server erstellen. Verbinden Sie sich hierzu über `ssh` mit dem Server und geben Sie Folgendes ein:

```
up2date &
```

Sie werden nun aufgefordert, das root-Passwort für den Server einzugeben. Anschließend erscheint **Red Hat Update Agent**, und Sie können Ihre Pakete auf dem Server aktualisieren, als ob Sie direkt vor Ihrem Rechner sitzen würden.

17.5.2. Port Forwarding

Mit SSH können Sie unsichere TCP/IP Protokolle via Port Forwarding sichern. Bei dieser Technik wird der SSH-Server zu einer verschlüsselten Verbindung zum SSH-Client.

Beim Port Forwarding wird ein lokaler Port auf einem Client zu einem remote Port auf dem Server gemappt. Mit SSH können Sie jeden Port des Servers auf jeden Port des Clients übertragen; die Portnummern müssen hierfür nicht übereinstimmen.

Um einen TCP/IP Port Forwarding Kanal zu erstellen, der nach Verbindungen im lokalen Host sucht, verwenden Sie folgenden Befehl:

```
ssh -L local-port:remote-hostname:remote-port username@hostname
```

Anmerkung

Für das Einrichten des Port-Forwarding auf Ports unterhalb 1024 Zylindern müssen Sie als root angemeldet sein.

Wenn Sie zum Beispiel Ihre E-Mails auf einem Server mit dem Namen `mail.example.com` mithilfe von POP3 über eine verschlüsselte Verbindung abrufen möchten, verwenden Sie folgenden Befehl:

```
ssh -L 1100:mail.example.com:110 mail.example.com
```

Nachdem der Port Forwarding Channel zwischen dem Client und dem Mailserver eingerichtet wurde, können Sie einen POP3-Mail-Client anweisen, Port 1100 auf dem localhost für das Abrufen neuer E-Mails zu verwenden. Alle an Port 1100 gesendeten Anforderungen werden auf diese Weise sicher an den Server `mail.example.com` weitergeleitet.

Wenn `mail.example.com` keinen SSH-Serverdaemon ausführt, Sie sich jedoch an einem anderen Rechner im gleichen Netzwerk anmelden können, können Sie dennoch SSH verwenden, um einen Teil der Verbindung zu sichern. Hierzu ist ein anderer Befehl notwendig:

```
ssh -L 1100:mail.example.com:110 other.example.com
```

In diesem Beispiel werden POP3-Anfragen von Port 1100 des Client-Rechners über die SSH-Verbindung auf Port 22 an den SSH-Server `other.example.com` weitergeleitet. Anschließend verbindet sich `other.example.com` mit Port 110 auf `mail.example.com`, so dass Sie neue E-Mails abrufen können. Beachten Sie, dass bei Verwendung dieser Methode nur die Verbindung zwischen dem Client-System und dem `other.example.com`-SSH-Server sicher ist.

Dies kann sehr nützlich sein, wenn Sie Informationen sicher über Netzwerk-Firewalls übertragen möchten. Wenn die Firewall so konfiguriert ist, dass SSH-Kommunikationen über den Standardport (22) erfolgen, die Übertragung über andere Ports jedoch gesperrt ist, ist eine Verbindung zwischen zwei Rechnern mit gesperrten Ports weiterhin möglich, indem die Meldungen über eine festgesetzte SSH-Verbindung zwischen diesen Rechnern übermittelt werden.

Anmerkung

Die Verwendung von Port Forwarding für das Weiterleiten von Verbindungen ermöglicht es jedem Benutzer des Client-Servers, sich mit diesem Service zu verbinden. Wird das Client-System kompromittiert, hat ein Angreifer auch Zugang zum Forwarding Service.

Systemadministratoren, die um das Port Forwarding besorgt sind, können diese Funktionalität auf dem Server deaktivieren, indem sie einen `No` Parameter für die Zeile `AllowTcpForwarding` in der Datei `/etc/ssh/sshd_config` angeben und den `sshd`-Service neu starten.

17.6. Anfordern von SSH für Fernverbindungen

Für ein effektives SSH dürfen Sie keine unsicheren Verbindungsprotokolle wie Telnet und FTP verwenden. Andernfalls wird das Passwort eines Benutzers mithilfe von SSH für eine Sitzung zwar geschützt, kann jedoch später durch eine Anmeldung bei Telnet erfasst werden.

Einige Dienste zum Deaktivieren enthalten:

- `telnet`
- `rsh`
- `rlogin`
- `vsftpd`

Deaktivieren Sie unsichere Verbindungsmethoden Ihres Systems mithilfe des Befehlszeilenprogramms `chkconfig`, des ncurses-basierten Programms **ntsysv** oder der grafischen Applikation **Services Configuration Tool** (`redhat-config-services`). Alle diese Tools erfordern root-Zugriff.

Weitere Informationen über Runlevels und das Konfigurieren von Diensten mit `chkconfig`, **ntsysv** und **Services Configuration Tool** finden Sie im Kapitel *Zugriffskontrolle zu Diensten* des *Red Hat Enterprise Linux Handbuch zur System-Administration*.

17.7. Zusätzliche Ressourcen

Weitere Informationen zu SSH finden Sie in den folgenden Ressourcen.

17.7.1. Installierte Dokumentation

- Das Verzeichnis `/usr/share/doc/openssh-<version-number>/` — Ersetzen Sie `<version-number>` mit der Version Ihres OpenSSH-Pakets. Dieses Verzeichnis enthält ein README mit grundlegenden Informationen über das OpenSSH Projekt, und eine Datei mit dem Namen `RFC.nroff` mit allgemeinen Informationen über das SSH-Protokoll.
- SSH-bezogene man-Seiten — Es gibt eine Vielzahl von man-Seiten für die verschiedenen Applikationen und Konfigurationsdateien für SSH. Im folgenden finden Sie eine Liste der bedeutenderen man-Seiten.

  Client Applikationen

  - `man ssh` — Beschreibt, wie dieser Befehl zur Verbindung mit einem SSH-Server verwendet werden kann.
  - `man scp` — Beschreibt, wie dieser Befehl zum Kopieren von Dateien von und auf einem SSH-Server verwendet werden kann.
  - `man sftp` — Beschreibt, wie dieser Befehl zum interaktiven Kopieren von Dateien von und auf einem SSH-Server verwendet werden kann.

  Server Applikationen

  - `man sshd` — Beschreibt die zur Verfügung stehenden Befehlszeilenoptionen für den SSH-Server.

  Konfigurationsdateien

  - `man ssh_config` — Beschreibt das Format und die Optionen, die innerhalb der Konfigurationsdatei für SSH-Clients zur Verfügung stehen.
  - `man sshd_config` — Beschreibt das Format und die Optionen, die innerhalb der Konfigurationsdatei für SSH-Server zur Verfügung stehen.

17.7.2. Nützliche Webseiten

- http://www.openssh.com — Die OpenSSH FAQ Seite, Bugreports, Mailinglisten, Projektziele und eine technische Erklärung der Sicherheitseigenschaften.
- http://www.openssl.org — Die OpenSSL FAQ Seite, Mailinglisten, und eine Beschreibung des Projektziels.
- http://www.freessh.org — SSH-Client Software für andere Plattformen.

17.7.3. Bücher zum Thema

- *Red Hat Enterprise Linux Handbuch zur System-Administration* Red Hat, Inc. — Das Kapitel *OpenSSH* beschreibt die Einrichtung eines SSH-Servers und die Verwendung der SSH-Client Software, die mit der OpenSSH-Toolsuite ausgeliefert wird. Desweiteren wird beschrieben, wie ein RSA (oder DSA) Schlüsselpaar erstellt wird, das passwortloses Anmelden ermöglicht.

IV. Anhang

Inhaltsverzeichnis

A. Allgemeine Parameter und Module..... 263

redhat

Anhang A.

Allgemeine Parameter und Module

Dieser Anhang soll *einige* der möglichen Parameter erklären, die für bestimmte, häufig verwendete Hardware-*Treiber*[1], die unter Red Hat Enterprise Linux Kernel-*Module* genannt werden. In den meisten Fällen sind diese zusätzlichen Parameter nicht notwendig, da der Kernel das Gerät bereits ohne sie verwenden kann. Es könnte jedoch vorkommen, dass zusätzliche Modul-Parameter notwendig sind, damit ein Gerät richtig arbeitet, oder wenn Sie die Standardparameter für das Gerät überschreiben möchten.

Während der Installation verwendet Red Hat Enterprise Linux eine eingeschränkte Untergruppe von Gerätetreibern, um eine stabile Installationsumgebung zu erzeugen. Obwohl das Installationsprogramm die Installation auf vielen verschiedenen Typen von Hardware unterstützt, sind manche Treiber (einschließlich der Treiber für SCSI-Adapter, Netzwerkkarten und viele CD-ROMs) nicht im Installations-Kernel integriert. Stattdessen sind sie als Module verfügbar, die während dem Bootvorgang vom Benutzer geladen werden müssen. Weitere Informationen über zusätzliche Kernel-Module während des Installationsprozesses finden Sie im Abschnitt über alternative Bootmethoden im Kapitel *Schritte für den erfolgreichen Start* im *Red Hat Enterprise Linux Installationshandbuch*.

Nach Abschluss der Installation besteht eine Unterstützung für eine große Anzahl von Geräten durch Kernel-Module.

Wichtig

Red Hat bietet eine große Anzahl nicht unterstützter Gerätetreiber in einer Reihe von Paketen, nämlich: `kernel-unsupported-<kernel-version>`, `kernel-smp-unsupported-<kernel-version>`, und `kernel-hugemem-unsupported-<kernel-version>`. Ersetzen Sie `<kernel-version>` mit der Version des Kernels, der auf dem System installiert ist. Diese Pakete werden vom Red Hat Enterprise Linux Installationsprogramm nicht installiert, und diebereitgestellten Module werden von Red Hat, Inc. nicht unterstützt.

A.1. Spezifizieren der Modulparameter

In einigen Situationen kann es notwendig sein, Parameter für ein Modul beim Laden desselben anzugeben, damit es richtig funktioniert.

Wenn Sie zum Beispiel für eine Intel Ether Express/100 Karte volle Duplex-Kapazität bei einer Verbindungsgeschwindigkeit von 100Mbps ermöglichen wollen, laden Sie den `e100` Treiber mit der `e100_speed_duplex=4` Option.

Achtung

Wenn ein Parameter Kommas beinhaltet, achten Sie darauf, dass Sie nach dem Komma *KEIN* Leerzeichen setzen.

1. zur Verfügung stehen. Unter einem Treiber versteht man Software, die Ihrem Linux System die Verwendung bestimmter Hardware-Geräte ermöglicht. Ohne den Treiber kann der Kernel mit den zugefügten Geräten nicht richtig kommunizieren

A.2. SCSI-Parameter

Hardware	Modul	Parameter
3ware Storage Controller	`3w-xxxx.o`	
NCR53c810/820/720, NCR53c700/710/700-66	`53c7,8xx.o`	
Adaptec AACRAID	`aacraid.o`	
Adaptec 28xx, R9xx, 39xx AHA-284x, AHA-29xx, AHA-394x, AHA-398x, AHA-274x, AHA-274xT, AHA-2842, AHA-2910B, AHA-2920C, AHA-2930/U/U2, AHA-2940/W/U/UW/AU/, U2W/U2/U2B/, U2BOEM, AHA-2944D/WD/UD/UWD, AHA-2950U2/W/B, AHA-3940/U/W/UW/, AUW/U2W/U2B, AHA-3950U2D, AHA-3985/U/W/UW, AIC-777x, AIC-785x, AIC-786x, AIC-787x, AIC-788x , AIC-789x, AIC-3860	`aic7xxx.o`	
ICP RAID Controller	`gdth.o`	
IBM ServeRAID	`ips.o`	
AMI MegaRAID 418, 428, 438, 466, 762	`megaraid.o`	
Qlogic 1280	`qla1280.o`	

Tabelle A-1. SCSI-Parameter

A.3. Ethernet-Parameter

Wichtig

Die meisten modernen Ethernet-basierten Netzwerk-Schnittstellen-Karten (NICs), erfordern keine Modul-Parameter um Einstellungen zu ändern. Diese können Anstelle mit `ethtool` oder `mii-tool` konfiguriert werden. Nur wenn der Versuch mit diesen Tools fehlschlägt, sollten Modul-Parameter angepasst werden.

Zu Information über die Verwendung dieser Tools, sehen Sie die man-Seiten von `ethtool` und `mii-tool`.

Hardware	Modul	Parameter

Hardware	Modul	Parameter
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	full_duplex= *0* ist ausgeschaltet *1* ist eingeschaltet
>RTL8139, SMC EZ Karte Fast Ethernet, RealTek Karten, die RTL8129 oder RTL8139 Fast Ethernet Chipsets verwenden.	`8139too.o`	
Intel Ether Express/100-Treiber	`e100.o`	e100_speed_duplex=*X* *Wenn X* = 0 = automatisches Finden Geschwindigkeit und Duplex 1 = 10Mbps, half duplex 2 = 10Mbps, full duplex 3 = 100Mbps, half duplex 4 = 100Mbps, full duplex
Intel EtherExpress/1000 Gigabit	`e1000.o`	
Intel i82557/i82558 PCI EtherExpressPro-Treiber	`eepro100.o`	
NatSemi DP83815 Fast Ethernet	`natsemi.o`	
AMD PCnet32 und AMD PCnetPCI	`pcnet32.o`	
SIS 900/701G PCI Fast Ethernet	`sis900.o`	
ThunderLAN	`tlan.o`	
Digital 21x4x Tulip PCI-Ethernetkarten SMC EtherPower 10 PCI(8432T/8432BT) SMC EtherPower 10/100 PCI(9332DST) DEC EtherWorks 100/10 PCI(DE500-XA) DEC EtherWorks 10 PCI(DE450) DEC QSILVER's, Znyx 312 etherarray Allied Telesis LA100PCI-T Danpex EN-9400, Cogent EM110	`tulip.o`	io=*I/O_Port*
VIA Rhine PCI Fast Ethernetkarten mit VIA VT86c100A Rhine-II PCI oder 3043 Rhine-I D-Link DFE-930-TX PCI 10/100	`via-rhine.o`	

Tabelle A-2. Ethernet-Modulparameter

A.3.1. Verwendung mehrerer Ethernet-Karten

Sie können auf einem Rechner mehrere Ethernet-Karten benutzen. Für jede Karte muss eine `alias` und, möglicherweise, eine `options` Zeile `/etc/modules.conf` vorhanden sein. Für weitere Informationen siehe Kapitel *Kernel-Module* im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Weitere Informationen zur Verwendung mehrerer Ethernet-Karten finden Sie unter *Linux Ethernet-HOWTO* unter der URL http://www.redhat.com/mirrors/LDP/HOWTO/Ethernet-HOWTO.html.

A.3.2. Die Kanal-Verbindungsmodule

Red Hat Enterprise Linux ermöglicht den Administratoren, die NICs in einem einzigen Kanal zusammenzubinden, indem das `bonding` Kernel-Modul und eine spezielle Schnittstelle, die Kanal-Verbindungsschnittstelle, verwendet wird. Die Kanalverbindung macht es möglich, dass zwei oder mehrere Netzwerk-Schnittstellen wie eine einzige agieren. Damit wird die Bandbreite simultan erhöht und dDatenfreiraum geschaffen.

Um eine Kanalverbindung zwischen mehreren Netzwerk-Schnittstellen herzustellen, muss der Administrator folgende Schritte ausführen:

1. Fügen Sie die folgende Zeile zu `/etc/modules.conf` hinzu:
   `alias bond<N> bonding`

   Ersetzen Sie Replace `<N>` mit der Schnittstellennummer z.B. `0`. Für jede konfigurierte Kanalverbindungs-Schnittstelle muss es einen korrespondierenden Eintrag in `/etc/modules.conf` geben.
2. Konfigurieren Sie eine Kanalverbindungs-Schnittstelle wie inAbschnitt 8.2.3 angegeben.
3. Um die Leistung zu verbessern, justieren Sie die verfügbaren Moduloptionen und stellen Sie fest, welche Kombination am besten funktioniert. Achten Sie besonders auf die `miimon` oder `arp_interval` und die `arp_ip_target` Parameter. Unter Abschnitt A.3.2.1 finden Sie eine Auflistung aller verfügbaren Funktionen.
4. Platzieren Sie die bevorzugten Moduloptionen nach dem Testen in `/etc/modules.conf`.

A.3.2.1. `bonding` Modul-Befehle

Bevor Sie die Einstellungen des `bonding` Modules beenden, wäre es günstig, zu testen, welche Einstellungen am besten funktionieren. Öffnen Sie hierfür einen Shell Prompt als Root und schreiben Sie:

```
tail -f /var/log/messages
```

Öffnen Sie einen weiteren Shell Prompt und verwenden Sie den `/sbin/insmod` Befehl, um das `bonding` Module mit anderen Parametern zu laden. Beobachten Sie dabei, ob der Kernel Fehlermeldungen ausgibt.

Der `/sbin/insmod` Befehl wird in folgendem Format ausgegeben:

```
/sbin/insmod bond<N> <parameter=value>
```

Ersetzen Sie `<N>` mit der Nummer der Verbindungs- Schnittstelle. Ersetzen Sie `<parameter=value>` durch eine Liste der gewüschten Paramter für die Schnittstelle (mit Leerstellen-Trennung).

Wenn Sie sich davon überzeugt haben, dass keine Fehler auftreten bzw. dass die Leistung der Verbindungs-Schnittstelle in Ordnung ist, fügen Sie die passenden `bonding` Modul-Parameter zu `/etc/modules.conf` hinzu.

Im Folgenden eine Liste der verfügbaren Parameter für das `bonding` Modul:

- `mode=` — Bestimmt eine der vier Richtlinien, die für das `bonding` Modul erlaubt sind. Folgende Werte sind für diesen Parameter zugelassen:
  - `0` — Legt eine allgemeingültige Richtlinie für die Fehlertoleranz und die Lastenverteilung fest. Die Übertragungen werden eine nach der anderen auf jeder verbundenen Nebenschnittstelle empfangen und versendet. Auf der ersten verfügbaren wird begonnen.
  - `1` — Legt eine Richtlinie für Aktiv-Datensicherung bei der Fehlertoleranz fest. Die Übertragungen werden über die erste verfügbare verbundene Nebenschnittstelle empfangen und versendet. Eine weitere verbundene Nebenschnittstelle wird nur dann verwendet, wenn die aktive verbundene Nebenschnittstelle versagt.
  - `2` — Legt eine XOR (exklusiv-oder) Richtlinie für die Fehlertoleranz und die Lastenverteilung fest. Mit dieser Methode vergleicht die Schnittstelle die MAC-Adressen der eingehenden Anfragen mit der MAC-Adresse für eine der Neben-NICs. Wenn diese Verbindung aufrecht ist, werden die Übertragungen eine nach der anderen, beginnend bei der ersten verfügbaren Schnittstelle, ausgesendet.
  - `3` — Legt eine allgemeingültige Richtlinie für die Fehlertoleranz und die Lastenverteilung fest. Die Übertragungen werden eine nach der anderen auf jeder verbundenen Nebenschnittstelle ausgesendet, beginnend mit der ersten verfügbaren.

- `miimon=` — Legt in Millisekunden fest, wie oft die MII-Verbindung beobachtet werden soll. Das ist dann wichtig, wenn eine hohe Verfügbarkeit gefragt ist, denn MII kann feststellen, ob die NIC akitv ist. Um zu überprüfen, ob der Treiber für eine bestimmte NIC das MII-Tool unterstützt, geben Sie den folgenden Befehl als Root ein:
  `ethtool <interface-name> | grep "Link detected:"`

  Ersetzen Sie bei diesem Befehl *<interface-name>* mit dem Namen der Geräte-Schnittstelle, z.B. `eth0`, nicht der `bond` Schnittstelle. Wenn MII unterstützt wird, zeigt der Befehl an:
  `Link detected: yes`

  Wenn Sie eine Verbindungs-Schnittstelle für hohe Verfügbarkeit verwenden, muss das Modul von jeder NIC MII unterstützen.

  Wenn Sie den Wert auf `0` setzen (Standardeinstellung), wird diese Funktion abgeschaltet. Wenn Sie die Einstellung konfigurieren, ist `100` ein guter Anfangspunkt für diesen Parameter.
- `downdelay=` — Legt in Millisekunden fest, wie lange nach einem Verbindungsversagen gewartet werden soll, bevor die Verbindung deaktiviert wird. Der Wert muss ein Vielfaches des Wertes betragen, der im`miimon` Parameter bestimmt wurde. Standardmäßig ist dieser Wert auf `0` eingestellt, was die Funktion deaktiviert.
- `updelay=` — Legt in Millisekunden fest, wie lange gewartet werden soll, bevor eine Verbindung aktiviert wird. Der Wert muss ein Vielfaches des Wertes betragen, der im `miimon` Parameter bestimmt wurde. Der Wert ist standardmäßig auf `0` gestellt, was die Funktion deaktiviert.
- `arp_interval=` — Legt in Millisekunden fest, wie oft ARP-Beobachtung eintritt.

  Wenn Sie diese Einstellung in `mode 0` oder `2` (die zwei Modi zum Lastenausgleich) verwenden, muss der Netzwerk-Schalter so konfiguriert sein, dass er die Pakete gleichmäßig über die NICs verteilt. Weitere Informationen zu dieser Funktion finden Sie unter`/usr/src/linux-2.4/Documentation/networking/bonding.txt` [2].

2. Dieses Dokument wird mit dem `kernel-source` Paket installiert.

Der Wert ist standardmäßig auf `0` eingestellt, was die Funktion deaktiviert.

- `arp_ip_target=` — Legt die Ziel-IP-Adresse von ARP-Anfragen fest, wenn der `arp_interval` Parameter aktiviert ist. In einer Liste mit Kommatrennung können bis zu 16 IP-Adressen festgelegt werden.
- `primary=` — Bestimmt den Namen der Schnittstelle des primären Gerätes z. B. `eth0`. Das `primary` Gerät ist die erste der verbundenen Schnittstellen, die verwendet wird. Sie wird nicht aufgelassen, außer wenn sie versagt. Diese Einstellung ist vor allem dann hilfreich, wenn eine NIC in der verbundenen Schnittstelle schneller ist und daher eine größere Last übernehmen kann.

  Diese Einstellung ist nur dann gültig, wenn sich die verbundene Schnittstelle in Aktiv-Datensicherungs-Modus befindet. Siehe `/usr/src/linux-2.4/Documentation/networking/bonding.txt`[2] für weitere Informationen.
- `multicast=` — Bestimmt einen Ganzzahlen-Wert für den Typ der gewünschten Multicast-Unterstützung.

  Zugelassene Werte für diesen Parameter sind:

  - `0` — Deaktiviert die Multicast-Unterstützung.
  - `1` — Aktiviert Multicast-Unterstützung, aber nur auf der aktiven Nebenschnittstelle.
  - `2` — Aktiviert Multicast-Unterstützung auf allen Nebenschnittstellen (Standardeinstellung).

Wichtig

Es ist notwendig, dass entweder die `arp_interval` und `arp_ip_target` oder `miimon` Parameter festgelegt werden. Wenn dies verabsäumt wird, kann die Leistung des Netzwerkes abfallen, wenn eine Verbindung versagt.

Für ausführliche Anweisungen bezüglich verbundener Schnittstellen, siehe `/usr/src/linux-2.4/Documentation/networking/bonding.txt`[2].

2. Dieses Dokument wird mit dem `kernel-source` Paket installiert.
2. Dieses Dokument wird mit dem `kernel-source` Paket installiert.

Stichwortverzeichnis

Symbols

/boot/-Verzeichnis, 26
/dev/-Verzeichnis, 26
/etc/-Verzeichnis, 26
/etc/named.conf
  (Siehe BIND)
/etc/pam.conf, 201
  (Siehe auch PAM)
/etc/pam.d, 201
  (Siehe auch PAM)
/etc/sysconfig/ Verzeichnis, 30
/etc/sysconfig/Verzeichnis
  (Siehe sysconfig Verzeichnis)
/initrd/ Verzeichnis, 30
/lib/-Verzeichnis, 26
/lib/security/, 201
  (Siehe auch PAM)
/lib64/security/, 201
  (Siehe auch PAM)
/mnt/-Verzeichnis, 26
/opt/-Verzeichnis, 27
/proc Dateisystem
  /proc/apm, 47
  /proc/bus Verzeichnis, 63
  /proc/cmdline, 47
  /proc/cpuinfo, 47
  /proc/devices
    Blockgeräte, 48
    Zeichen-Geräte, 48
  /proc/dma, 49
  /proc/driver Verzeichnis, 63
  /proc/execdomains, 49
  /proc/fb, 50
  /proc/filesystems, 50
  /proc/fsVerzeichnis, 64
  /proc/ide Verzeichnis, 64
    Geräte-Verzeichnisse, 65
  /proc/interrupts, 50
  /proc/iomem, 51
  /proc/ioports, 52
  /proc/irq Verzeichnis, 66
  /proc/isapnp, 52
  /proc/kcore, 53
  /proc/kmsg, 53
  /proc/ksyms, 53
  /proc/loadavg, 54
  /proc/locks, 54
  /proc/mdstat, 54
  /proc/meminfo, 55
  /proc/misc, 56
  /proc/modules, 56
  /proc/mounts, 57
  /proc/mtrr, 57
  /proc/net Verzeichnis, 66
  /proc/partitions, 58
  /proc/pci
    Anzeige mitlspci, 58
  /proc/scsi Verzeichnis, 67
  /proc/self Verzeichnis, 63
  /proc/slabinfo, 59
  /proc/stat, 59
  /proc/swaps, 60
  /proc/sys Verzeichnis, 68, 78
    (Siehe auch sysctl)
    /proc/sys/devVerzeichnis, 69
    /proc/sys/fsVerzeichnis, 70
    /proc/sys/kernel/sysrq
      (Siehe System Request Key)
    /proc/sys/kernelVerzeichnis, 71
    /proc/sys/vm Verzeichnis, 75
    netVerzeichnis, 74
  /proc/sysrq-trigger, 60
  /proc/sysvipc Verzeichnis, 77
  /proc/tty Verzeichnis, 77
  /proc/uptime, 60
  /proc/version, 60
  Dateien anzeigen in, 45
  Dateien in, top-level, 46
  Dateien ändern in, 46, 68, 78
  eingeführt, 45
  Prozesse-Verzeichnisse, 61
  Unterverzeichnisse in, 61
  zusätzliche Ressourcen, 79
    hilfreiche Websites, 79
    installierte Dokumentation, 79
/proc/-Verzeichnis, 27
/procVerzeichnis
  (Siehe /proc Dateisystem)
/sbin/-Verzeichnis, 27
/usr/-Verzeichnis, 27
/usr/local/-Verzeichnis directory, 28
/var/-Verzeichnis, 29
/var/lib/rpm/ Verzeichnis, 30
/var/spool/up2date/ Verzeichnis, 30

A

aboot, 3
AccessFileName
  Apache-Konfigurationsanweisung, 152
Action
  Apache-Konfigurationsanweisung, 158
AddDescription
  Apache-Konfigurationsanweisung, 157
AddEncoding
  Apache-Konfigurationsanweisung, 157
AddHandler
  Apache-Konfigurationsanweisung, 158
AddIcon
  Apache-Konfigurationsanweisung, 156
AddIconByEncoding
  Apache-Konfigurationsanweisung, 156
AddIconByType
  Apache-Konfigurationsanweisung, 156
AddLanguage
  Apache-Konfigurationsanweisung, 157
AddType
  Apache-Konfigurationsanweisung, 157
Alias
  Apache-Konfigurationsanweisung, 155
Allow
  Apache-Konfigurationsanweisung, 152
AllowOverride
  Apache-Konfigurationsanweisung, 151
Anhalten, 9
  (Siehe auch shutdown)
Apache
  (Siehe Apache HTTP Server)
Apache HTTP Server
  1.3
    Migrieren in 2.0, 133
  2.0
    Dateisystemänderungen, 132
    Merkmale von, 131
    Migrieren aus 1.3, 133
    MRM-spezifische Anweisungen, 146
    Packetänderungen, 132
  Anhalten, 143
  Ausfü:hren ohne Sicherheit, 163
  Einführung, 131
  Konfiguration, 145
  Log-Dateien
    /var/log/httpd/error_log, 145
    Format von, 154
    Gemeinsames Logdatei-Format, 154, 154
    Problembehebung mit, 145, 146
    Verwende Log-Analyzer-Tools mit, 153
  Migrieren in 2.0, 133
    Bind-Adressen und Ports, 133
    DSO Support, 135
    Entfernte Anweisungen, 135
    Fehlerdokumente, 137
    Indizieren der Verzeichnisse, 137
    Inhaltsverhandlung, 137
    Konfiguration des virtuellen Host, 138
    LDAP, 142
    Logging, 136
    Modulsystemänderungen, 138
    mod_auth_db, 140
    mod_auth_dbm, 140
    mod_include, 140
    mod_perl, 141
    mod_proxy, 139
    mod_ssl, 139
    PHP, 142
    Server-Pool Größe, 134
    UserDir Anweisung, 136
  Multi-Processing Module
    Aktiviere worker MPM, 134
    prefork, 134
    worker, 134
  neu laden, 143
  neu starten, 143
  Problembehebung, 145
  Server-Statusberichte, 159
  Starten, 143
  zusätzliche Ressourcen, 165
    hilfreiche Websites, 165
    zusätzliche Bücher, 165
Apache HTTP Server-Module, 162
APXS Apache-Dienstprogramm, 163
authconfig
  und LDAP, 194, 195
autofs, 126
  (Siehe auch NFS)

B

Basic Input/Output System
  (Siehe BIOS)
Benutzer
  /etc/passwd, 82
  Einführung, 81
  Standard, 82
  Tools zur Verwaltung von
    User Manager, 81
    useradd, 81
  UID, 81
  Zusätzliche Informationsquellen, 87
    Bücher zum gleichen Thema, 88
    Installierte Dokumentation, 87
Benutzereigene Gruppen
    (Siehe Gruppen)
  und gemeinsame Verzeichnisse, 85
Berkeley Internet Name Domain
  (Siehe BIND)

BIND
Allgemeine Fehler, 184
Einführung, 167, 167
Features, 182
DNS-Erweiterungen, 183
IPv6, 184
Mehrere Ansichten, 183
Sicherheit, 183
Konfiguration von
Beispiel eines zone Statements, 173
Beispiele für Zone-Dateien, 178
Resource-Records der Zone-Datei, 176
umgekehrte Auflösung von Namen, 179
Zone-Dateien-Direktiven, 175
Konfigurationsdateien
/etc/named.conf, 168, 169
/var/named/-Verzeichnis, 168
Zone-Dateien, 175
named-Daemon, 168
Nameserver
Definition von, 167
Nameserver-Typen
Caching-Only, 168
Forwarding, 168
Master, 168
Slave, 168
rndc-Programm, 180
/etc/rndc.conf, 181
Befehlszeilenoptionen, 182
named für Verwendung konfigurieren, 180
Schlüssel konfigurieren, 181
Root-Nameserver
Definition von, 167
Zonen
Definition von, 167
Zusätzliche Ressourcen, 184
Bücher zum Thema, 186
Hilfreiche Webseiten, 186
Installierte Dokumentationen, 185
BIOS
Definition von, 1
(Siehe auch boot process)
Blockgeräte, 48
(Siehe auch /proc/devices)
Definition von, 48
Bootloader, 11, 19
(Siehe auch GRUB)
(Siehe auch LILO)
Definition von, 11
Typen
ELILO, 11
GRUB, 11
LILO, 11
OS/400, 11
YABOOT, 11
z/IPL, 11
Bootprozess, 1, 1
(Siehe auch boot loaders)
Direktes Laden, 11
für x86, 1
Phasen, 1, 1
/sbin/init-Befehl, 4
BIOS, 1
Bootloader, 2
EFI-Shell, 1
Kernel, 4
Verkettetes Laden, 11
BrowserMatch
Apache-Konfigurationsanweisung, 158

C

Cache-Konfigurationsanweisungen für Apache, 160
CacheNegotiatedDocs
Apache-Konfigurationsanweisung, 153
Caching-Only Nameserver
(Siehe BIND)
CGI-Skripts
außerhalb ScriptAlias, 158
externe Ausführung zulassen cgi-bin, 150
Channel-Bonding
Schnittstelle
Konfiguration von, 111
chkconfig, 9
(Siehe auch services)
CustomLog
Apache-Konfigurationsanweisung, 154

D

Dateien, Proc-Dateisystem
Anzeigen von Dateien, 45, 78
ändern, 46, 78
Dateisystem
Hierarchie, 25
Organisation, 25
Standard, 25
Struktur, 25
virtuelles
(Siehe /proc Dateisystem)
DefaultIcon
Apache-Konfigurationsanweisung, 156
DefaultType
Apache-Konfigurationsanweisung, 153
Denial of Service
Verhinderung mit xinetd, 224
(Siehe auch xinetd)
Denial of Service Angriff, 74
(Siehe auch /proc/sys/net/ directory)
Definition von, 74
Deny

Apache-Konfigurationsanweisung, 152
Desktop-Umgebungen
(Siehe XFree86)
Directory
Apache-Konfigurationsanweisung, 150
DirectoryIndex
Apache-Konfigurationsanweisung, 152
Display Manager
(Siehe XFree86)
DNS, 167
(Siehe auch BIND)
Einführung, 167
DocumentRoot
Apache-Konfigurationsanweisung, 150
gemeinsam verwendete ändern, 164
ändern, 163
Dokumentation
die geeignete finden, ii
Einsteiger, iii
Bücher, iv
Newsgroups, iv
Webseiten, iii
erfahrene Benutzer, iv
Guru, v
DoS
(Siehe Denial of Service)
DoS Angriff
(Siehe Denial of Service Angriff)
drag and drop, viii
DSOs
laden, 163

E

EFI-Shell
Definition von, 1
(Siehe auch boot process)
Einführung, i
ELILO, 3, 11
(Siehe auch boot loaders)
Epoch, 59
(Siehe auch /proc/stat)
Definition von, 59
ErrorDocument
Apache-Konfigurationsanweisung, 158
ErrorLog
Apache-Konfigurationsanweisung, 153
Erweiterbare Firmware-Schnittstellen-Shell
(Siehe EFI-Shell)
Ethernet
(Siehe Netzwerk)
Ethernet-Module
(Siehe Kernel-Module)
Execution Domains, 49
(Siehe auch /proc/execdomains)
Definition von, 49
ExtendedStatus
Apache-Konfigurationsanweisung, 148

F

Feedback
Kontaktadressen, ix
FHS, 25, 25
(Siehe auch file system)
(Siehe auch file system)
Forwarding Nameserver
(Siehe BIND)
Framebuffer-Gerät, 50
(Siehe auch /proc/fb)
FrontPage, 143
fstab, 126
(Siehe auch NFS)

G

Geräte, lokal
Besitzrechte über, 208
(Siehe auch PAM)
GNOME, 90
(Siehe auch XFree86)
Group
Apache-Konfigurationsanweisung, 149
GRUB, 2, 11
(Siehe auch boot loaders)
(Siehe auch boot loaders)
Befehle, 16
Bootprozess, 11
Definition von, 11
Funktionen, 12
Installieren, 13
Konfigurationsdatei
/boot/grub/grub.conf, 18
Struktur, 18
Menükonfigurationsdatei, 18
Anweisungen, 18
Oberflächen, 15
Befehlszeile, 15
Menü, 15
Menüeintrag-Editor, 15
Reihenfolge der, 16
Rolle im Bootprozess, 2
Runlevels ändern mit, 15, 22
Terminologie, 13
Dateien, 14
Geräte, 13
Root-Dateisystem, 15
zusätzliche Ressourcen, 23
Bücher zu diesem Thema, 24
hilfreiche Websites, 23

installierte Dokumentationen, 23
grub.conf, 18
(Siehe auch GRUB)
Gruppen
Benutzereigene, 85
Einführung, 81
Gemeinsame Verzeichnisse, 85
GID, 81
Standard, 83
Tools zur Verwaltung von
groupadd, 81, 85
redhat-config-users, 85
User Manager, 81
Zusätzliche Informationsquellen, 87
Bücher zum gleichen Thema, 88
Installierte Dokumentation, 87

H

HeaderName
Apache-Konfigurationsanweisung, 157
Herunterfahren, 9
(Siehe auch halt)
Hierarchie, Dateisystem, 25
HostnameLookups
Apache-Konfigurationsanweisung, 153
Hosts-Zugriffsdateien
(Siehe TCP Wrappers)
hosts.allow
(Siehe TCP Wrappers)
hosts.deny
(Siehe TCP Wrappers)
httpd.conf
(Siehe Konfigurationsanweisungen, Apache)
Hugepages
Konfiguration von, 75

I

IfDefine
Apache-Konfigurationsanweisung, 149
ifdown, 115
IfModule
Apache-Konfigurationsanweisung, 146
ifup, 115
Include
Apache-Konfigurationsanweisung, 148
IndexIgnore
Apache-Konfigurationsanweisung, 157
IndexOptions
Apache-Konfigurationsanweisung, 156
init-Befehl, 4
(Siehe auch boot process)
auf Runlevel zugreifen, 8
Konfigurationsdateien
/etc/inittab, 7
Rolle im Bootprozess, 4
(Siehe auch boot process)
Runlevels
Verzeichnisse für, 7
SysV init
Definition von, 7
ip6tables
Einführung, 239
Kontrollskripte
Neustart, 237
Panik, 237
Speichern, 237
Start, 237
Status, 237
stop, 237
ipchains
(Siehe iptables)
IPsec
(Siehe Netzwerk)
iptables
/sbin/iptables-restore, 236
/sbin/iptables-save, 236
Chains
Ziel, 227
Grundlagen der Paket-Filterung, 227
Konfigurationsdateien
/etc/sysconfig/iptables, 236
/etc/sysconfig/iptables-config, 238
/etc/sysconfig/iptables.save, 236
Kontrollskripte
Neustart, 237
Panik, 237
Speichern, 236, 237
Start, 237
Status, 237
stop, 237
Optionen, 229
Auflistung, 236
Befehle, 230
Parameter, 231
Struktur von, 229
Ziel, 235
Protokolle
ICMP, 233
TCP, 232
UDP, 233
Regelliste, 227
Regeln speichern, 236
Tabellen, 227
Vergleich mit ipchains, 228
Zusätzliche Informationsquellen, 239
hilfreiche Websites, 239
Installierte Dokumentation, 239
Überblick, 227
Übereinstimmungsoptionen, 232

Module, 234

K

Kanalverbindung
Modul-Befehle, 266
Modul-Konfiguration, 266
KDE, 90
(Siehe auch XFree86)
KeepAlive
Apache-Konfigurationsanweisung, 146
KeepAliveTimeout
Apache-Konfigurationsanweisung, 146
Kerberos
Authentifizierungs-Server (AS), 244
Client einrichten, 247
Definition von, 241
Funktionsweise, 244
Key Distribution Center (KDC), 244
Nachteile von, 241
Server einrichten, 246
Terminologie, 242
Ticket Granting Server (TGS), 244
Ticket Granting Ticket (TGT), 244
und PAM, 245
Vorteile von, 241
zusätzliche Ressourcen, 248
hilfreiche Webseiten, 250
Installierte Dokumentation, 248
Kernel
Rolle im Bootprozess, 4
Kernel-Module
Einführung, 263
Ethernet-Module
mehrere Karten unterstützen, 266
Parameter, 264
Modulparameter
spezifizieren, 263
SCSI-Module
Parameter, 264
Typen, 263
Konfiguration
Apache HTTP Server, 145
virtuelle Hosts, 163
Konfigurationsanweisungen, Apache, 145
AccessFileName, 152
Action, 158
AddDescription, 157
AddEncoding, 157
AddHandler, 158
AddIcon, 156
AddIconByEncoding, 156
AddIconByType, 156
AddLanguage, 157
AddType, 157
Alias, 155
Allow, 152
AllowOverride, 151
BrowserMatch, 158
CacheNegotiatedDocs, 153
CustomLog, 154
DefaultIcon, 156
DefaultType, 153
Deny, 152
Directory, 150
DirectoryIndex, 152
DocumentRoot, 150
ErrorDocument, 158
ErrorLog, 153
ExtendedStatus, 148
für Cache-Funktionalitäten, 160
Group, 149
HeaderName, 157
HostnameLookups, 153
IfDefine, 149
IfModule, 146
Include, 148
IndexIgnore, 157
IndexOptions, 156
KeepAlive, 146
(Siehe auch KeepAliveTimeout)
Problembehebung, 146
KeepAliveTimeout, 146
LanguagePriority, 157
Listen, 148
LoadModule, 148
Location, 159
LogFormat
Format-Optionen, 154
LogLevel, 154
MaxClients, 147
MaxKeepAliveRequests, 146
MaxRequestsPerChild, 147
MaxSpareServers, 147
MaxSpareThreads, 147
MinSpareServers, 147
MinSpareThreads, 147
NameVirtualHost, 160
Options, 151
Order, 151
PidFile, 145
Proxy, 159
ProxyRequests, 159
ProxyVia, 159
ReadmeName, 157
Redirect, 155
ScriptAlias, 155
ServerAdmin, 149
ServerName, 149
ServerRoot, 145
ServerSignature, 155

SetEnvIf, 161
SSL-Konfiguration, 161
StartServers, 147
ThreadsPerChild, 148
Timeout, 146
TypesConfig, 153
UseCanonicalName, 150
User, 149
UserDir, 152
VirtualHost, 161
Konventionen
Dokument, v
Kopieren und Einfügen von Text
beim Verwenden von X, viii
kwin, 90
(Siehe auch XFree86)

L

LanguagePriority
Apache-Konfigurationsanweisung, 157
LDAP
Applikationen
ldapadd, 189
ldapdelete, 189
ldapmodify, 189
ldappasswd, 189
ldapsearch, 189
OpenLDAP Suite, 189
slapadd, 189
slapcat, 189
slapcat-gdbm, 189
slapd, 189
slapindex, 189
slappasswd, 189
slurpd, 189
Utilities, 189
Authetifizierung unter Verwendung von, 194
/etc/ldap.conf bearbeiten, 194
/etc/nsswitch.conf bearbeiten, 194
/etc/openldap/ldap.conf bearbeiten, 194
authconfig, 194
Clients einrichten, 194
Pakete, 194
PAM, 195
slapd.conf bearbeiten, 194
Client-Applikationen, 191
Daemons, 189
Definition, 187
Konfigurationsdateien
/etc/ldap.conf, 191
/etc/openldap/ldap.conf, 191
/etc/openldap/schema/-Verzeichnis, 191, 191
/etc/openldap/slapd.conf, 191, 193
LDAPv2, 187
LDAPv3, 187
LDIF
Format, 188
mit Apache HTTP Server verwenden, 190
mit NSS verwenden, 190
mit PAM verwenden, 190
mit PHP4 verwenden, 190
OpenLDAP Funktionen, 187
setting up, 192
Umwandeln der 1.x Verzeichnisse, 196
Umwandeln älterer Verzeichnisse, 196
Terminologie, 188
Upgrade von Verzeichnissen, 196
Vorteile, 187
Zusätzliche Ressourcen, 197
Bücher zum Thema, 198
hilfreiche Websites, 198
installierte Dokumentationen, 197
ldapadd Befehl, 189
(Siehe auch LDAP)
ldapdelete Befehl, 189
(Siehe auch LDAP)
ldapmodify Befehl, 189
(Siehe auch LDAP)
ldappasswd Befehl, 189
(Siehe auch LDAP)
ldapsearch Befehl, 189
(Siehe auch LDAP)
Lightweight Directory Access Protocol
(Siehe LDAP)
LILO, 2, 11
(Siehe auch boot loaders)
(Siehe auch boot loaders)
Bootprozess, 20
Definition von, 19
Konfigurationsdatei
/etc/lilo.conf, 21
Rolle im Bootprozess, 2
Runlevels ändern mit, 22
zusätzliche Ressourcen, 23
Bücher zu diesem Thema, 24
hilfreiche Websites, 23
installierte Dokumentationen, 23
lilo.conf, 21
(Siehe auch LILO)
Listen
Apache-Konfigurationsanweisung, 148
LoadModule
Apache-Konfigurationsanweisung, 148
Location
Apache-Konfigurationsanweisung, 159
LogFormat
Apache-Konfigurationsanweisung, 154
LogLevel
Apache-Konfigurationsanweisung, 154
lspci, 58

M

Master Boot Record
  (Siehe MBR)
  (Siehe MBR)
Master Nameserver
  (Siehe BIND)
Maus
  verwenden, viii
MaxClients
  Apache-Konfigurationsanweisung, 147
MaxKeepAliveRequests
  Apache-Konfigurationsanweisung, 146
MaxRequestsPerChild
  Apache-Konfigurationsanweisung, 147
MaxSpareServers
  Apache-Konfigurationsanweisung, 147
MaxSpareThreads
  Apache-Konfigurationsanweisung, 147
MBR
  Definition von, 1, 1
    (Siehe auch boot loaders)
    (Siehe auch boot process)
metacity, 90
  (Siehe auch XFree86)
MinSpareServers
  Apache-Konfigurationsanweisung, 147
MinSpareThreads
  Apache-Konfigurationsanweisung, 147
Module
      (Siehe Kernel-Module)
      (Siehe Kernel-Module)
  Apache
    Ihr eigenes, 163
    laden, 163
  standard, 162
Modulparameter
  (Siehe Kernel-Module)
mwm, 90
  (Siehe auch XFree86)

N

named-Daemon
  (Siehe BIND)
named.conf
  (Siehe BIND)
Nameserver
  (Siehe BIND)
NameVirtualHost
  Apache-Konfigurationsanweisung, 160
netfilter
  (Siehe iptables)
Netzwerk
  Befehle
    /sbin/ifdown, 115
    /sbin/ifup, 115
    /sbin/service network, 115
  Funktionen, 116
  Konfiguration, 108
  Schnittstellen, 108
    Alias, 112
    Channel-Bonding, 111
    Clone, 112
    Dialup, 113
    Ethernet, 108
    IPsec, 110
  Skripts, 107
  Zusätzliche Ressourcen, 116
Netzwerk-Dateisystem
  (Siehe NFS)
NFS
  Anhalten, 122
  Bedingter Neustart, 122
  Client
    /etc/fstab, 126
    autofs, 126
    Konfiguration, 126
    Mount-Optionen, 128
  Einführung, 119
  Erforderliche Dienste, 120
  Neu laden, 122
  Neu starten, 122
  portmap, 120
  Server-Konfiguration, 122
    /etc/exports, 123
    exportfs Befehl, 125
  Sicherheit, 128
    Dateiberechtigungen, 129
    Host-Zugriff, 129
  Starten, 122
  Status, 122
  TCP, 119
  UDP, 119
  Wie es funktioniert, 119
  zusätzliche Informationsquellen, 130
    installierte Dokumentation, 130
    Nützliche Websites, 130
    zusätzliche Literatur, 130
NIC-Module
  (Siehe Kernel-Module)
ntsysv, 9
  (Siehe auch services)

O

Objekte, dynamisch gemeinsam verwendet
(Siehe DSOs)
OpenLDAP
(Siehe LDAP)
OpenSSH, 251
(Siehe auch SSH)
Konfigurationsdateien, 254
Options
Apache-Konfigurationsanweisung, 151
Order
Apache-Konfigurationsanweisung, 151
OS/400, 11
(Siehe auch boot loaders)

P

Paket-Filterung
(Siehe iptables)
PAM
Beispiele für Konfigurationsdateien, 204
Definition von, 201
Kerberos und, 245
Konfigurationsdateien, 201
Module, 202
Argumente, 204
Erstellen, 206
Komponenten, 202
Schnittstellen, 202
Speicherort, 203
stapeln>, 202, 204
pam_console
Definition von, 208
pam_timestamp
Anweisungen, 208
Authentication Icon und, 207
Definition von, 207
zerstöre Timestamps, 207
pam_timestamp_check
Zerstöre Timestamp mit, 207
Servicedateien, 201
Shadow-Passwörter, 204
Steuer-Flags, 203
Vorteile, 201
zusätzliche Ressourcen, 209
hilfreiche Websites, 210
installierte Dokumentationen, 209
pam_console
(Siehe PAM)
pam_timestamp
(Siehe PAM)
pam_timestamp_check
(Siehe PAM)
Passwort, 204
(Siehe auch PAM)
Shadow-Passwörter, 204
Passwörter
Shadow, 86
PidFile
Apache-Konfigurationsanweisung, 145
Pluggable Authentication Modules
(Siehe PAM)
portmap, 120
(Siehe auch NFS)
NFS, 121
rpcinfo, 121
Status, 122
prefdm
(Siehe XFree86)
Problembehebung
Fehlerprotokoll, 153
Programme
zum Zeitpunkt des Bootens ausführen, 7
Proxy
Apache-Konfigurationsanweisung, 159
proxy server, 159, 160
ProxyRequests
Apache-Konfigurationsanweisung, 159
ProxyVia
Apache-Konfigurationsanweisung, 159
public_html directories, 152

R

rc.local
ändern, 7
rc.serial, 7
(Siehe auch setserial command)
ReadmeName
Apache-Konfigurationsanweisung, 157
Red Hat Enterprise Linux-spezifische Dateispeicherstellen
/etc/sysconfig/, 30
(Siehe auch sysconfig directory)
/var/lib/rpm/, 30
/var/spool/up2date/, 30
Redirect
Apache-Konfigurationsanweisung, 155
Root-Nameserver
(Siehe BIND)
rpcinfo, 121
Runlevels
(Siehe init-Befehl)
Konfiguration, 9
(Siehe auch services)
zum Zeitpunkt des Bootens ändern, 22
ändern mit GRUB, 15

S

ScriptAlias
  Apache-Konfigurationsanweisung, 155
SCSI-Module
  (Siehe Kernel-Module)
serielle Schnittstellen
  (Siehe setserial Befehl)
Server-seitige Includes, 151, 157
ServerAdmin
  Apache-Konfigurationsanweisung, 149
ServerName
  Apache-Konfigurationsanweisung, 149
ServerRoot
  Apache-Konfigurationsanweisung, 145
ServerSignature
  Apache-Konfigurationsanweisung, 155
Services
  mit chkconfig konfigurieren, 9
  mit ntsysv konfigurieren, 9
  mit Services Configuration Tool konfigurieren, 9
Services Configuration Tool, 9
  (Siehe auch services)
SetEnvIf
  Apache-Konfigurationsanweisung, 161
setserial Befehl
  Konfigurieren, 7
Shadow
  (Siehe Passwort)
Shadow Passwörter
  Überblick, 86
Sicherheit
  Apache ausführen ohne, 163
Slab Pools
  (Siehe /proc/slabinfo)
slapadd Befehl, 189
  (Siehe auch LDAP)
slapcat Befehl, 189
  (Siehe auch LDAP)
slapcat-gdbm Befehl, 189
  (Siehe auch LDAP)
slapd Befehl, 189
  (Siehe auch LDAP)
slapindex Befehl, 189
  (Siehe auch LDAP)
slappasswd Befehl, 189
  (Siehe auch LDAP)
Slave Nameserver
  (Siehe BIND)
slurpd Befehl, 189
  (Siehe auch LDAP)
SSH-Protokoll protocol, 251
  Abfolge des Verbindungsaufbaus, 252
  Anfordern für Fernanmeldung, 257
  Authentifizierung, 254
  Konfigurationsdateien, 254
  Merkmale von, 251
  Port Forwarding, 256
  Schichten von
    Kanäle, 254
    Transportschicht, 253
  Sicherheitsrisiken, 251
  unsichere Protokolle und, 257
  Version 1, 252
  Version 2, 252
  X11 Forwarding, 256
  Zusätzliche Ressourcen, 258
    Bücher zum Thema, 259
    Installierte Dokumentation, 258
    Nützliche Webseiten, 259
SSL-Konfiguration, 161
StartServers
  Apache-Konfigurationsanweisung, 147
startx
  (Siehe XFree86)
sysconfig Verzeichnis
  /etc/sysconfig/amd, 32
  /etc/sysconfig/apm-scripts/-Verzeichnis, 43
  /etc/sysconfig/apmd, 32
  /etc/sysconfig/authconfig, 32
  /etc/sysconfig/cbq/-Verzeichnis, 43
  /etc/sysconfig/clock, 33
  /etc/sysconfig/desktop, 34
  /etc/sysconfig/devlabel, 34
  /etc/sysconfig/dhcpd, 34
  /etc/sysconfig/firstboot, 34
  /etc/sysconfig/gpm, 35
  /etc/sysconfig/harddisks, 35
  /etc/sysconfig/hwconf, 35
  /etc/sysconfig/init, 36
  /etc/sysconfig/ipt6ables-config, 36
  /etc/sysconfig/iptables, 37
  /etc/sysconfig/irda, 37
  /etc/sysconfig/keyboard, 38
  /etc/sysconfig/kudzu, 38
  /etc/sysconfig/mouse, 38
  /etc/sysconfig/named, 39
  /etc/sysconfig/netdump, 39
  /etc/sysconfig/network, 39
  /etc/sysconfig/ntpd, 40
  /etc/sysconfig/pcmcia, 40
  /etc/sysconfig/radvd, 41
  /etc/sysconfig/rawdevices, 41
  /etc/sysconfig/redhat-config-securitylevel , 41
  /etc/sysconfig/redhat-config-users, 41
  /etc/sysconfig/redhat-logviewer, 41
  /etc/sysconfig/rhn/-Verzeichnis, 44
  /etc/sysconfig/samba, 41
  /etc/sysconfig/sendmail, 42
  /etc/sysconfig/spamassassin, 42
  /etc/sysconfig/squid, 42
  /etc/sysconfig/tux, 42

/etc/sysconfig/vncservers, 42
/etc/sysconfig/xinetd, 43
Dateien in, 31
Verzeichnisse in, 43
zusätzliche Informationen, 31
Zusätzliche Ressourcen, 44
Installierte Dokumentation, 44
sysconfig-Verzeichnis
/etc/sysconfig/iptables, 236
/etc/sysconfig/network-scripts/-Verzeichnis, 43
(Siehe auch network)
/etc/sysconfig/networking/-Verzeichnis, 43
sysconfigVerzeichnis
/etc/sysconfig/network-scripts/ Verzeichnis, 107
sysctl
Konfigurieren mit /etc/sysctl.conf, 78
Prüfen /proc/sys/, 78
SysRq
(Siehe System Request Key)
System Request Key
aktivieren, 68
System-Request-Key
Definition von, 68
Timing setzen, 71
SysV init
(Siehe init-Befehl)

T

TCP Wrappers, 219
(Siehe auch xinetd)
Definition von, 211
Einführung, 211
Konfigurationsdateien
/etc/hosts.allow, 211, 212
/etc/hosts.deny, 211, 212
Expansionen, 218
Formatierungsregeln in, 213
Hosts-Zugriffsdateien, 212
Log-Option, 216
Operatoren, 216
Option-Felder, 216
Optionen der Zugriffskontrolle, 217
Patterns, 215
Shell-Befehl Option, 217
spawn Option, 217
twist Option, 217
Wildcards, 214
Vorteile, 212
zusätzliche Ressourcen, 224
Bücher zum Thema, 225
installierte Dokumentation, 224
nützliche Websites, 225
ThreadsPerChild
Apache-Konfigurationsanweisung, 148
Timeout
Apache-Konfigurationsanweisung, 146
TLB-Cache
(Siehe Hugepages)
Treiber
(Siehe Kernel-Module)
twm, 90
(Siehe auch XFree86)
TypesConfig
Apache-Konfigurationsanweisung, 153

U

Unverschlüsselte Web-Server
deaktivieren, 165
UseCanonicalName
Apache-Konfigurationsanweisung, 150
User
Apache-Konfigurationsanweisung, 149
UserDir
Apache-Konfigurationsanweisung, 152
users
private HTML-Verzeichnisse, 152

V

Verzeichnisse
/boot/, 26
/dev/, 26
/etc/, 26
/lib/, 26
/mnt/, 26
/opt/, 27
/proc/, 27
/sbin/, 27
/usr/, 27
/usr/local/, 28
/var/, 29
VirtualHost
Apache-Konfigurationsanweisung, 161
Virtuelle Dateien
(Siehe /proc Dateisystem)
virtuelle Hosts
konfigurieren, 163
Listen-Befehl, 164
namensbasiert, 163
Options, 151
Server-seitige Includes, 157
Virtuelles Dateisystem
(Siehe /proc Dateisystem)

W

Webmaster
E-Mail-Adresse für, 149
Window Manager
(Siehe XFree86)

X

X
(Siehe XFree86)
X Window System
(Siehe XFree86)
X.500
(Siehe LDAP)
X.500 Lite
(Siehe LDAP)
XFree86
/etc/X11/XF86Config
Boolesche Werte für, 91
Device, 96
DRI, 97
Einführung, 91
Files Abschnitt, 93
InputDevice Abschnitt, 94
Module Abschnitt, 94
Monitor, 95
Screen, 97
Section Tag, 91
ServerFlags Abschnitt, 92
ServerLayout Abschnitt, 92
Struktur, 91
Desktop-Umgebungen
GNOME, 90
KDE, 90
Dienstprogramme
X Configuration Tool, 89
Display Manager
Definition, 101
gdm, 101
kdm, 101
Konfiguration der vorgezogenen, 101
prefdm Skript, 101
xdm, 101
Einführung, 89
Fonts
Core X Font-Subsystem, 99
Einführung, 98
Fontconfig, 98
Fontconfig, Fonts hinzufügen, 99
FreeType, 98
X Font Server, 99
X Render Extension, 98
xfs, 99
xfs Konfiguration, 99
xfs, Fonts hinzufügen, 100
Xft, 98
Konfigurationsdateien
/etc/X11/ Verzeichnis, 91
/etc/X11/XF86Config, 91
Optionen, 91
Serveroptionen, 91
Runlevel
3, 101
5, 101
Runlevels, 101
Window Manager
kwin, 90
metacity, 90
mwm, 90
twm, 90
X Server, 89
Funktionen, 89
XFree86, 89
X-Clients, 89, 90
Desktop-Umgebungen, 90
startx command, 101
Window Manager, 90
xinit, 101
Zusätzliche Ressourcen, 102
Installierte Dokumentation, 103
Nützliche Webseiten, 103
Zusätzliche Literatur, 103
xinetd, 219
(Siehe auch TCP wrappers)
DoS-Angriffen und, 224
Einführung, 211, 219
Konfigurationsdateien, 219
/etc/xinetd.conf, 219
/etc/xinetd.d/ directory, 220
Bindungs-Optionen, 223
Protokoll-Optionen, 219, 220, 221
Ressourcen-Management-Optionen, 224
Umleitungs-Optionen, 223
Zugriffskontroll-Optionen, 221
Verhältnis zu TCP-Wrapper, 221
zusätzliche Ressourcen
Bücher zum Thema, 225
installierte Dokumentation, 224
nützliche Websites, 225
xinit
(Siehe XFree86)

Y

YABOOT, 11
(Siehe auch boot loaders)

Z

z/IPL, 11
    (Siehe auch boot loaders)
Zeichen-Geräte, 48
        (Siehe auch /proc/devices)
    Definition von, 48
Zugriffskontrolle, 211

Colophon

Die Handbücher wurden im Format DocBook SGML v4.1 erstellt. Die HTML- und PDF-Formate werden unter Verwendung benutzerdefinierter DSSSL Stylesheets und benutzerdefinierten Jade Wrapper Scripts angelegt. Die DocBook SGML-Dateien wurden in **Emacs** mithilfe von PSGML Mode geschrieben.

Garrett LeSage schuf das Design der Grafiken für Meldungen (Anmerkung, Tipp, Wichtig, Achtung und Warnung). Diese dürfen frei zusammen mit der Red Hat-Dokumentation vertrieben werden.

Das Team der Red Hat-Produktdokumentation besteht aus:

Sandra A. Moore — Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Installationshandbuch für x86, Itanium™ und AMD64 Architekturen* Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Installationshandbuch für IBM® eServer™ iSeries™ und IBM® eServer™ pSeries™ Architekturen* Co-Autorin des *Red Hat Enterprise Linux Schrittweise Einführung*

Tammy Fox — Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Handbuch zur System-Administration*; Co-Autorin des *Red Hat Enterprise Linux Installationshandbuch für x86, Itanium™ und AMD64 Architekturen*; Co-Autorin des *Red Hat Enterprise Linux Sicherheitshandbuch*; Co-Autorin des *Red Hat Enterprise Linux Schrittweise Einführung*; Autorin/Bearbeiterin der benutzerdefinierten DocBook Stylesheets und Skripte

Edward C. Bailey — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Introduction to System Administration*; Verantwortlicher Autor/Bearbeiter der *Release Notes*; Co-Autor des *Red Hat Enterprise Linux Installationshandbuch für x86, Itanium™ und AMD64 Architekturen*

Johnray Fuller — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Referenzhandbuch*; Co-Autor/Co-Bearbeiter des *Red Hat Enterprise Linux Sicherheitshandbuch*; Co-Autor des *Red Hat Enterprise Linux Introduction to System Administration*

John Ha — Verantwortlicher Autor/Bearbeiter des *Red Hat Cluster Suite Configuring and Managing a Cluster*; Verantwortlicher Autor/Bearbeiter des *Red Hat Glossary*; Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Installationshandbuch für IBM® S/390® und IBM® eServer™ zSeries® Architekturen*; Co-Autor/Co-Bearbeiter des *Red Hat Enterprise Linux Sicherheitshandbuch*; Co-Autor des *Red Hat Enterprise Linux Introduction to System Administration*; Co-Autor des *Red Hat Enterprise Linux Schrittweise Einführung*

Das Red Hat-Team verantwortlich für Übersetzungen besteht aus:

Jean-Paul Aubry — Französisch

David Barzilay — Portugisisch (Brasilien)

Bernd Groh — Deutsch

James Hashida — Japanisch

Michelle Ji-yeen Kim — Koreanisch

Yelitza Louze — Spanisch

Noriko Mizumoto — Japanisch

Nadine Richter — Deutsch

Audrey Simons — Französisch

Francesco Valente — Italienisch

Sarah Saiying Wang — Einfaches Chinesisch

Ben Hung-Pin Wu — Traditionelles Chinesisch